NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE PROJECT REPORT

ADVANCED RESTRICTED AREA ENTRY CONTROL SYSTEM (ARAECS)

by

Team SSP
Cohort 311-124O

June 2014

Project Advisors: John M. Green
Daniel Burns

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Capstone Project Report

4. TITLE AND SUBTITLE ADVANCED RESTRICTED AREA ENTRY CONTROL SYSTEM (ARAECS)	**5. FUNDING NUMBERS**
6. AUTHOR(S) Cohort 311-124O/ Team SSP	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** UU

13. ABSTRACT (maximum 200 words)

The Navy requires a capability for effective and efficient entry control for restricted areas that house critical assets. This thesis describes an Advanced Restricted Area Entry Control System (ARAECS) to meet this requirement. System requirements were obtained from existing governing documentation as well as stakeholder inputs. A functional architecture was developed and then modeled using the Imagine That Inc. ExtendSim tool. Factors affecting ARAECS operation were binned into physical, technology, Concept of Operations (CONOPS), and noise. An Overall Measure of Effectiveness was developed and a Design of Experiments (DOE) was conducted to measure the affects of these factors on ARAECS performance.

The two main drivers were minimizing security violations while also maximizing personnel and vehicle throughput. Based on the modeling, an architecture was selected that best met system objectives—this architecture relied on the ability to pre-screen 40% of the workforce based on security clearance and thus subject them to reduced random screening. The architecture was documented using the Vitech CORE tool, and use cases were developed and documented. A test and evaluation plan was developed and discussed. Risk was then examined, including technical, schedule, and cost risks.

14. SUBJECT TERMS Advanced Restricted Area Entry Control System (ARAECS), system architecture, restricted area, entry control, contraband, functional architecture	**15. NUMBER OF PAGES** 175
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

ADVANCED RESTRICTED AREA ENTRY CONTROL SYSTEM (ARAECS)

Cohort 311-124O/Team SSP

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

Robert Appleton, Jose Casillas, Gregory Scales
Robert Green, and Melissa Niehoff

AND

MASTER OF SCIENCE IN ENGINEERING SYSTEMS

David Fitzgerald and David Ouellette

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Lead editor: David Fitzgerald

Reviewed by:

John M. Green	Daniel Burns
Project Advisor	Project Advisor

Accepted by:
Cliff Whitcomb
Systems Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Navy requires a capability for effective and efficient entry control for restricted areas that house critical assets. This report describes an Advanced Restricted Area Entry Control System (ARAECS) to meet this requirement. System requirements were obtained from existing governing documentation as well as stakeholder inputs. A functional architecture was developed and then modeled using the Imagine That Inc. ExtendSim tool. Factors affecting ARAECS operation were binned into physical, technology, Concept of Operations (CONOPS), and noise. An Overall Measure of Effectiveness was developed and a Design of Experiments (DOE) was conducted to measure the affects of these factors on ARAECS performance.

The two main objectives were minimizing security violations while also maximizing personnel and vehicle throughput. Based on the modeling, an architecture was selected that best met system objectives—this architecture relied on the ability to pre-screen 40% of the workforce based on security clearance and thus subject them to reduced random screening. The architecture was documented using the Vitech CORE tool, and use cases were developed and documented. A test and evaluation plan was developed and discussed. Risk was then examined, including technical, schedule, and cost risks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A	Architecture
AoA	Analysis of Alternatives
ARAECS	Advanced Restricted Area Entry Control System
CONOPS	Concept of Operations
DOD	Department of Defense
DoDAF	DOD Architecture Framework
DT&E	Developmental Test and Evaluation
ECP	Entry Control Point
EFFBD	Enhanced Functional Flow Block Diagram
F	Functional
FFC	Fleet Forces Command
I	Integration
IAW	In Accordance With
ICD	Initial Capability Document
IDEF	Integrated Definition
IPR	Interim Project Reviews
KPP	Key Performance Parameters
MCSF	Marine Corp Security Forces
MEF	Marine Expeditionary Forces
MOE	Measure of Effectiveness
MOP	Measure of Performance
MSSE	Masters of Science in Systems Engineering
M&S	Modeling and Simulation
NAC-LC	National Agency Check with Local Agency Check
NAVSEA	Naval Sea Systems Command
NPS	Naval Postgraduate School
OMOE	Overall Measurement of Effectiveness
OT&E	Operational Test and Evaluation
PACFLT	Pacific Fleet
PD	Preliminary Design

Pd	Probability of Detection
POC	Point of Contact
R	Review
S	Seconds
SoS	System of Systems
SS	Subsystem
SSBN	Nuclear Powered Ballistic Missile Submarine
SSP	Strategic Systems Programs
SSPINST	SSP Instruction
SWFLANT	Strategic Weapons Facility Atlantic
SWFPAC	Strategic Weapons Facility Pacific
SYS	System
TAD	Temporary Assigned Duty
TRL	Technology Readiness Level
WNY	Washington Navy Yard

EXECUTIVE SUMMARY

The Advanced Restricted Area Entry Control System (ARAECS) project addresses the following U.S. Navy mission need statement: The U.S. Navy requires a capability for efficient and effective entry control for restricted areas that house critical naval assets. This capstone examines a notional Navy Level 3 Restricted Area, a special type of industrial and refit zone that normally handles high value units such as aircraft carriers and ballistic missile submarines. The overall purpose of the project was to develop an architecture for the ARAECS that satisfies this requirement.

The ARAECS Team adopted an integrated architecture and modeling methodology, tied to defined requirements and measured through a weighted OMOE. Specific requirements were obtained from governing directives and are listed in detail in Appendix D. Additionally, the team elicited stakeholder input to identify requirements not provided by the governing directives. The process to execute the team's methodology is summarized as: (1) identify the required processes to accomplish the assigned mission; (2) allocate functions to the required processes; and (3) allocate objects to the required functions.

There are four principal security protocols that the ARAECS system must be able to accomplish:

- Validate badge and person. Each person who attempts entry into the restricted area must have a unique badge with corresponding picture identification. The badge must be valid (e.g., non-expired) and the person's identifying features must match the picture on the badge.
- Validate area authorities. Each person must be authorized access to the specific restricted area. ARAECS must only allow authorized individuals access into the restricted area.
- Screen for contraband. Each restricted area may have varying types of items that are prohibited. ARAECS must detect contraband prior to its introduction within the security area.

- Detect duress. Duress is defined as an individual who is compelled by force to willfully violate security requirements. ARAECS must not allow personnel under duress to enter the restricted area.

Additionally, ARAECS must perform its functions while accommodating a reasonable introduction of clients into the server. This was modeled through the arrival times and distributions that represents a two-shift workforce across a twenty-four hour period. ARAECS must also accommodate the introduction of vehicles into the restricted area while maintaining the four principal protocols. Security violators must be removed from the system though specific procedures for this are outside the scope of this capstone. ARAECS must be physically configured in a manner that supports the requirements. Examples of possible configuration options include different numbers of entry points and lanes that process personnel and vehicles.

ExtendSim8 was used to construct a model to allow the varying introduction of personnel and vehicles into queues to await individual entry to the restricted area. Once personnel and vehicles entered the restricted area they remained for approximately eight hours, simulating a typical work shift, then returned to the entry point and processed out. Model factors that influence performance were identified and then categorized according to the following: (1) uncontrollable factors (noise); (2) physical improvements, such as those that would require military construction; (3) technology improvements; and (4) human-based CONOPS improvements. A single response was developed for the model so that a Design of Experiments (DOE) technique could be used to track performance related factor variance.

The ARAECS model produced two measures of performance considered important in the customer ranking. The first was delay time while waiting to process through the ECP. The second was the number of security violators that are improperly processed. The customer stakeholder inputs indicated that lowering the number of security violations is more important than a shorter wait time.

These were combined into an Overall Measure of Effectiveness given by:

$$OMOE = \frac{(5000 + w_t)}{5000} n_{scc}{}^{1.7}$$

Full derivation of the OMOE can be found in Appendix B of this report.

The team conducted all DOE and statistical analysis with the MiniTab software suite. The initial DOE looked at a fractional factorial design made of 22 factors and two levels. Using the OMOE as the single response, thirteen of the original factors could be discarded as having no statistically significant impact on overall system performance.

The top two factors that screened in the DOE involved the rate of detailed search for personnel entry and the rate of random personnel checks. The detailed search is a more effective search, thus more detailed searches result in fewer security violations. Increasing the rate of random checks provides essentially the same result, so while these two factors screened at the top, they ultimately demonstrate very similar capabilities of the system. The team also conducted an analysis between the interactions of various factors. The interaction plot provided no real insights other than confirming that the rate of detailed search and the rate of the random check essentially illustrate the same effect.

Due to the fact that the ARAECS project is intended to be extensible to a diverse group of Navy locations, additional factor analysis was done by analyzing responses when the factor variance was constrained to either CONOPS or Physical. As a secondary reason to examine physical CONOPS, the team was interested in lowering the wait time as much as possible. Wait time must always be a consideration because the costs associated with unproductive wait time are a huge concern, not to mention the impact on industrial facility production and schedule.

In addition to the DOE factor analysis of physical and CONOPS, four initial variants were constructed based upon improving factors within the CONOPS, Technology, and Physical groupings that utilized static factor values based upon reasonable values. The OMOE computation remained the same as the DOE. An additional variant was constructed that utilized the best values from each of the three capability-type variants, which was known as the “Super.” The Super was analyzed as a comparison and end-point, i.e., a “best-case” OMOE.

None of the initial variants adequately addressed the MOPs, so the ARAECS Team revisited the DOE insights for an alternative solution that performed as well as the "Super Variant," but without maximizing all performance factors to achieve the desired responses for both precision and speed. The seed-capability for this improvement is in the detailed search factor. To address this, the team picked the DOD security clearance process as an institutionalized system that allows a security force to compare relative trustworthiness as a result of background checks and command monitoring. Utilizing the security clearance process, this "hybrid" ARAECS variant assumes that 40% of the typical workforce that enters the restricted area possesses at least a SECRET (National Agency Check with Local Agency Check (NAC-LC)-based) clearance. Personnel possessing a clearance are allowed to process through a separate ECP where they are given a passing visual search for gross contraband violations (e.g., visible weapons). Since there are no absolute guarantees, 5% of cleared personnel are still selected for random detailed screening.

Three separate variants of this "hybrid" ARAECS were modeled and the best performing version (Hybrid-B) was chosen as the basis for the ARAECS architecture. The Hybrid-B Variant is an integrated entry control system that utilizes a combination of manpower, physical control features, and technology to control personnel, validate entry requirements, and screen for contraband. It physically interfaces with an existing boundary system (i.e., perimeter fence) and electronically interfaces with an enrollment database. As shown by modeling, it is highly robust with respect to the rate of unauthorized entry and personnel requiring escort. Its defining feature is the pre-screening of personnel through the use of the DOD security clearance background checks in order to allocate the majority of detailed searches to personnel that are relatively unknown and thus represent a higher risk.

The team then developed representative use cases for personnel and vehicle entry to further define the architecure. Operational activity models were constructed which include the performers, organization, data flow between the performers, and a process compliant with requirements. The functional architecure was then developed, with decomposition down to Level 3. Enhanced Functional Flow Block Diagrams (EEFBD) were used to further describe system functionality.

The system test program was outlined based on five categories: (1) requirements testing, some of which can be verified through test and evaluation and some through audit; (2) safety testing to verify that the physical architecture is safe for use by both entrants and security personnel, (3) user interface testing which includes all testing associated with the human-machine interface, (4) operational testing including subsystem testing and system testing in a laboratory setting, and (5) field testing to verify the system works under field conditions (i.e., in the intended operational environment).

Finally, risk analysis is discussed, including risk characterization, risk tracking, and risk assessment. Candidate ARAECS technologies are described in detail in Appendix C. A summary of the team's technology readiness level (TRL) for each of these technologies is provided in the risk analysis section.

The team concludes that the proposed ARAECS architecture merits further study and analysis to determine if it could be applied to Strategic Systems Programs sites. Further areas of investigation include: identifying which candidate technologies should be incorporated into the system and determining if the OMOE could be refined to more specifically address different "levels" of security violations.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

On September 16, 2013, Aaron Alexis, an information technology specialist and support subcontractor to the Navy, smuggled a shotgun aboard the Washington Navy Yard (WNY). Allegedly operating under a grand delusion that he was being affected by extremely low frequency radio waves, he commenced a shooting spree within the Naval Sea Systems Command (NAVSEA) Headquarters that ended with the deaths of 13 people including him.

On March 24, 2014, Jeffrey Savage, a convicted felon who worked as a truck driver, gained entry to Norfolk Naval Station and walked onto the quarterdeck of USS Mahan (DDG 72), overpowered the petty officer of the deck, and took his weapon. He later used the weapon to kill a responding security officer, and was subsequently killed by other responding security forces.

In the first incident, media commentators immediately questioned how a clinically unstable person had access to sensitive government facilities and was able to smuggle the unauthorized weapon past the gate checkpoints at the WNY. In the second incident, there were questions about how the truck driver gained access to the naval station with his Transportation Security Administration–issued Transportation Worker Identity Credential, which the Navy reported was not sufficient to gain base access. Additionally, the truck driver was a convicted felon who had served prison time for both manslaughter and drug offenses.

Base access is a complex problem; the workforce largely arrives in a small time window each day, demands to be processed quickly through the checkpoint, and is rarely questioned upon entrance so long as each person presents valid entry credentials. The second incident showed that there are considerations beyond this: here the truck driver arrived at 11:30 pm and presented credentials reported to be insufficient to gain base access. He did not bring contraband onto the Naval Station; he gained access to his weapon by taking it from an individual authorized to have it.

The attack at WNY threatened and disrupted the Navy's intellectual capital by striking at the geographical heart of weapons system and ship design activities. The attack at Naval Station Norfolk illustrated that an individual gaining access to a U.S. Navy warship can cause tragic consequences even with no evident thought-out plan of attack, simply taking advantage of opportunities. These lone-wolf attackers, however, are a type of threat that must be considered at all Navy locations. Consequences of similar attacks against critical naval industrial facilities, ordnance processing, or ship berthing could have a calamitous effect on the Navy's operational posture, in turn degrading the United States' credibility and capability to project power and influence overseas.

Many Navy facilities have characteristics similar to those in the scenarios above: they employ active-duty servicemen, civilians, and contractors; they have thousands of workers reporting every day; and, finding a potential violent actor in possession of contraband (firearms, explosives, etc.) is tantamount to finding a needle in a haystack.

II. BACKGROUND

A. MISSION NEEDS STATEMENT

The Advanced Restricted Area Entry Control System (ARAECS) project addresses the following U.S. Navy mission need statement: *The U.S. Navy requires a capability for efficient and effective entry control for restricted areas that house critical naval assets.*

This project examines a notional Navy Level 3 Restricted Area, a special type of industrial and refit zone that normally handles high value units such as aircraft carriers and ballistic missile submarines. To avoid security classification concerns, no specific location was chosen. Because the members of the project team are all associated with Strategic Systems Programs (SSP), an SSBN operational area was used as the basis for analysis but the extensible architecture and conceptual design developed could be tailored for a wide variety of naval support activity locations.

B. PROJECT SCOPE

This project analyzes requirements within a socio-technological system that controls the authorized access of individuals into a Navy industrial-type restricted area. As this project is a part of a larger system-of-systems (SoS), the parent prime directive is: Deny unauthorized access to critical naval assets.

This project in context with the parent SoS is shown in Figure 1. The prime directive of this project’s support to the SoS is: Control authorized entry into restricted areas.

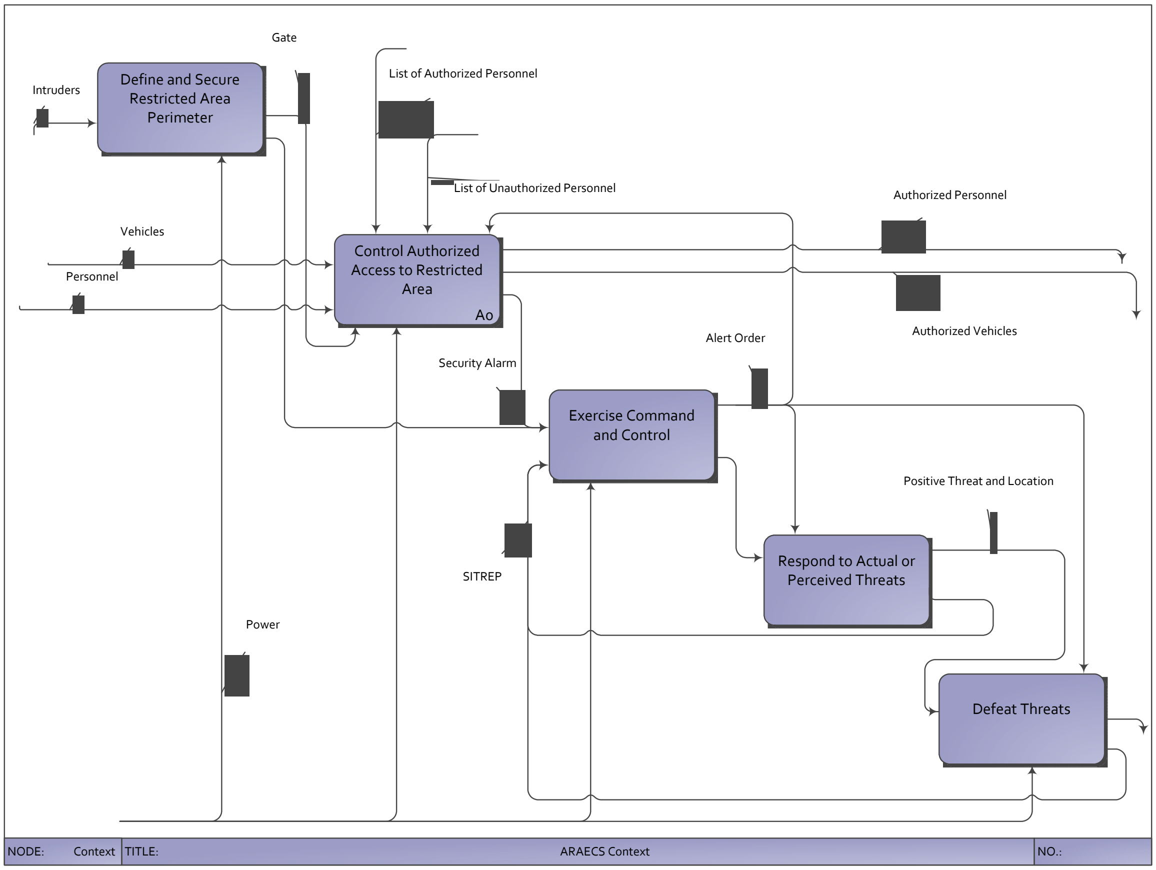

Gate
Intruders
Define and Secure Restricted Area Perimeter
List of Authorized Personnel
List of Unauthorized Personnel
Authorized Personnel
Vehicles
Personnel
Control Authorized Access to Restricted Area
Ao
Authorized Vehicles
Alert Order
Security Alarm
Exercise Command and Control
Positive Threat and Location
SITREP
Respond to Actual or Perceived Threats
Power
Defeat Threats
NODE:
Context
TITLE:
ARAECS Context
NO.:

Figure 1. Notional Context Diagram

The specific scope of this project focuses on personnel and vehicles entering a control point. The system must efficiently and effectively ascertain whether the personnel, vehicles, or other hand-carried equipment are authorized or present a threat. Authorized personnel and vehicles are allowed to proceed, but any contraband or unauthorized individuals will produce an alarm. Actions taken to respond to security alarms fall outside of the scope of this project.

(1) Threat Detection. A threat, in the context of this project, meets one of these three criteria:

- An individual, requesting entry into the restricted area, who lacks the required credentials (unauthorized individual) This is not necessarily a "bad actor" but may just be someone with an expired security badge or a badge with an administrative error (e.g., misspelling).

- An individual, requesting entry into the restricted area with required credentials, but attempting to introduce or remove unauthorized material (contraband)
- An individual, requesting entry into the restricted area without required credentials and attempting to introduce or remove unauthorized material (unauthorized individual with contraband)

For the purposes of this project, contraband will include:

- weapons, ammunition, or explosives
- flame-producing items (without a hotwork permit)
- knives with blades longer than 3 inches
- classified media without an authorized courier card
- photographic/video equipment without an authorized camera pass

(2) Threat Assessment. The method of threat assessment is a central aspect of the project's conceptual design. The project team considered manual, automated, and remote aspects of threat assessment including a combination of these various methods.

(3) Threat Response. Threat response and defeating the threat, to include the associated command and control, are outside the scope of this project. This project shall interface with the command and control system through a security alarm to the Command and Control system, which will trigger follow-on activities.

C. STAKEHOLDERS

Table 1 lists the project primary stakeholders. These stakeholders assisted the project team in helping to determine what is required of the solution used to fill the capability gap.

Stakeholders
Strategic Systems Programs (SSP)
II Marine Expeditionary Force (II MEF)
Fleet Forces Command / Pacific Fleet (FFC / PACFLT)
Strategic Weapons Facilities and MCSF Battalions • **Strategic Weapons Facility Atlantic (SWFLANT)** • **Strategic Weapons Facility Pacific (SWFPAC)** • **MCSF Battalion Kings Bay** • **MCSF Battalion Bangor**
Naval Postgraduate School (NPS)

Table 1. Project Primary Stakeholders

D. ROLES AND RESPONSIBILITIES

1. Team Member Roles

The Capstone project team was comprised of seven students who all work for SSP at SSP Headquarters at the WNY or at one of SSP's field activities, see Table 2. lists the individuals' names, roles, and responsibilities. Beyond these overall roles and responsibilities, everyone was also involved in working groups as needed and the creating of all necessary project artifacts, presentations, and reports.

Team Member	**Roles**	**Responsibilities**
David Fitzgerald	Team Lead	Liaison between team and stakeholders Direct team meetings Develop meeting agendas Present technical briefings
Robert Appleton	Systems Architect	Maintain Use Cases Develop system architecture (CORE) Maintain overall team CORE file Maintain M&S products (ExtendSim8) Maintain experimental data Derive and conduct OMOE analysis Perform Design of Experiments (DOE) Conduct Analysis of Alternatives (AoA) Interface and coordinate with stakeholders
Robert Green	Test Engineer and Scheduler	Develop test plans Coordinate and maintain team schedule Maintain and manage team project plan Perform technology research
David Ouellette	Systems Engineer	Perform technology research Maintain CONOPS
Gregory Scales	Systems Engineer	Draft stakeholder survey Coordinate research relating to AoA and AoA analysis Coordinate and Maintain Research Relating to Risk Analysis
Jose Casillas	Systems Analyst	Perform technology research
Melissa Niehoff	Cost Analyst and Team Secretary	Perform and maintain cost and risk analyses Compile team reports and presentations Coordinate and manage team discussion forums Provide team meeting minutes

Table 2. Team Member Roles and Responsibilities

2. Advisor Roles

The Capstone project team was supported by two advisors. Table 3 lists the advisor’s names, roles and responsibilities.

Advisors	Roles	Responsibilities
Professor John Green	Support Advisor	Provide insight and feedback based on System Engineering approach submitted by team. Providing consulting services and project expertise to team when requested by the team. Review and Approve the project at various milestones (IPR#1, IPR#2)
Professor Dan Burns	Support Advisor	Provide POC of possible Navy stakeholders Provide team with feedback on the Project Management Plan and Schedule Provide resources (travel funding, software licenses, etc.) as requested by the team and as available Review and Approve the project at various milestones (IPR#1, IPR#2, etc.)

Table 3. Advisor’s Roles and Responsibilities

III. METHODOLOGY

A. SYSTEMS ENGINEERING PROCESS

The DOD systems engineering process is a collection of technical and management processes applied through the life cycle. The following sub-sections describe this project's selected systems engineering process, known as the "Dual Vee" model. Figure 2 depicts the multi-axis approach of the Dual Vee, with each major step of development tied to a later stage of validation, and each entity decomposing into its own increasingly complex level of development.

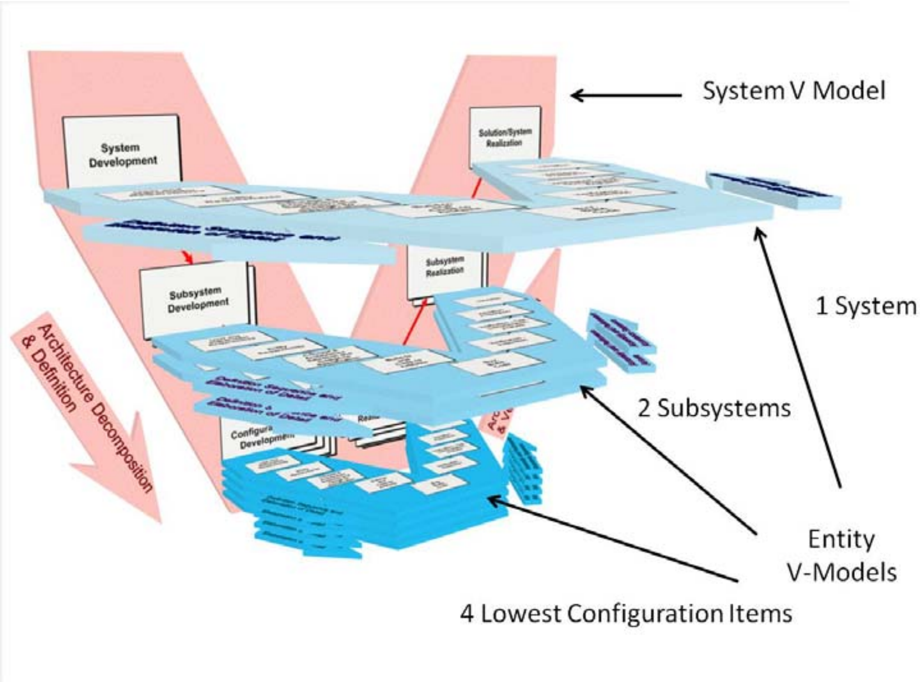


Figure 2. Dual-Vee Model of System Development (From Forsberg 2005)

1. Purpose

The purpose of this section is to document the tailored approach the team used with the Dual Vee in context of the project's scope—providing a firm technical foundation for system development. A rigorous technical planning process forces thoughtful consideration and debate, allows for integration and coordination of technical activities across all levels of management, and results in a sound systems engineering strategy commensurate with the program's technical issues, life cycle phasing, and overall objectives. The level of fidelity and emphasis documented here will evolve as the program progresses through its life cycle. This early developmental process can be disseminated to future program members and key stakeholders as required if the project moves forward toward detailed design and acquisition. It provides a common reference to achieve stakeholder insight regarding a program's planned technical approach. Figure 3 depicts one of the entity Vee breakouts from the Dual Vee.

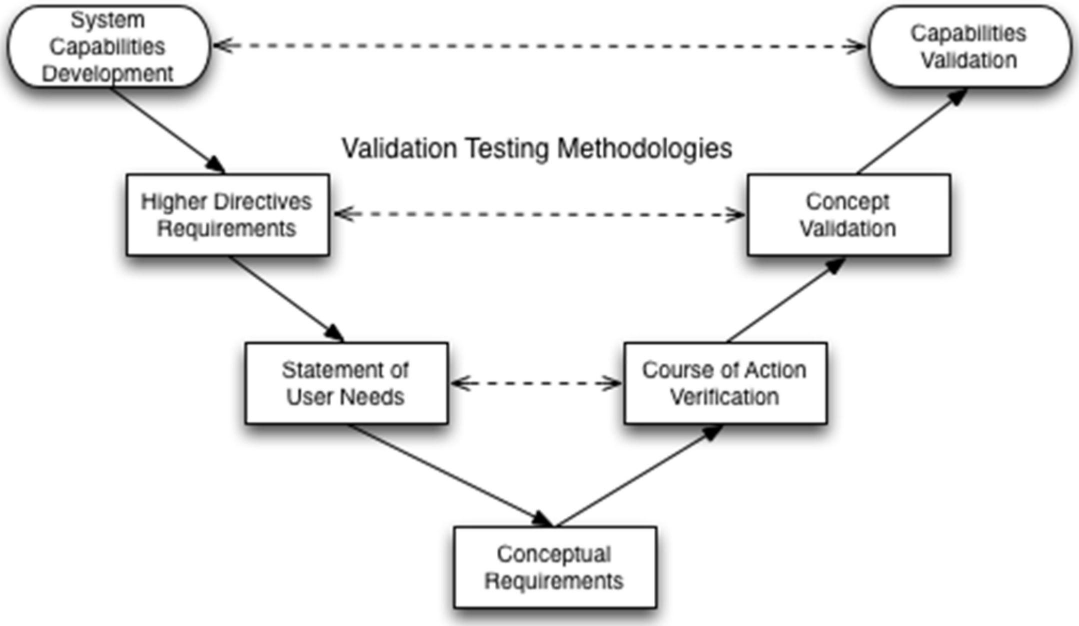

System Capabilities Development
Capabilities Validation
Validation Testing Methodologies
Higher Directives Requirements
Concept Validation
Statement of User Needs
Course of Action Verification
Conceptual Requirements

Figure 3. Entity Vee Approach Towards Requirements Development

2. Architecture

This project utilized the DOD Architecture Framework (DoDAF) to provide structure, process, and definition for organizing concepts, principles, assumptions, and terminology about operations and solutions into meaningful patterns. The DoDAF enables the sharing and reuse of architectural data and meets the goal of providing sufficient system definition to a future team that may engage in detailed design and acquisition (DODAF 2013).

3. System Requirements

High level system requirements are very important to establish early on in a project's life cycle. For the ARAECS, the system requirements were determined from both governing directives and a stakeholder analysis. Some of the high level operational requirements defined are: mission definition, performance and physical parameters, operational deployment or distribution, operational life cycle, utilization requirements, effectiveness factors, and environmental factors (Blanchard and Fabrycky 2011). The requirements are detailed in Appendix D, Systems Specification Document.

B. CONCEPT EXPLORATION

The team's Dual Vee System Engineering process began with the documented problem statement of increasing precision and efficiency for restricted area entry control. In this case, a need was identified where the Navy has industrial-level ship refit areas subject to stringent security requirements that often conflict with the production goals of throughput and constrained ship schedules. Security measures are frequently viewed as a cumbersome time-consuming process that detracts from overall operational efficiency. However, if the security forces fail in effective entry control, they could allow threats into the restricted area. The Navy needs a system that balances the required precise screening of individuals and vehicles, compliant with higher directives, while achieving to the maximum extent possible user needs/desires for effective and efficient operation.

Stakeholders were contacted to get their inputs into the project, and they provided operational restraints and constraints that were incorporated into the developed architecture. A stakeholder analysis was performed to determine which are the most important aspects and requirements of the system. This needs analysis, integrated with higher directive requirements, guided what and how the system needs to accomplish the project's prime directive and was used to develop the System Overall Method of Effectiveness (OMOE), discussed in detail in Appendix B.

1. Concept of Operations

The concept of operations is that individuals shall be subject to random detailed searches for contraband, as specified in system requirements. The facility shall leverage existing security clearances as an aspect of added trustworthiness—this was an insight gained from modeling and simulation, discussed in detail in section 3.6. Individuals with a security clearance are admitted entrance to the restricted area with fewer detailed searches conducted than those without security clearances, resulting in a much more efficient operation.

One person at a time is processed per lane at the entry control point (ECP). The person is required to have an enrolled smartcard including biometrics and a PIN. The person approaches the ECP and gets "buzzed" into the entrapment area, inserts the smart card, enters the PIN, and is scanned for biometrics. A detailed discussion of smart cards and biometrics is presented in Appendix C.

A vehicle driver enters the vehicle entrapment area and stops the vehicle, then shuts off the engine and opens all compartments for security inspection. Upon being ordered by the sentry, the driver gets into line with any vehicle passengers and processes in through the personnel ECP. The vehicle sentry searches the vehicle and secures any open compartments after searching them. After successful entry through the ECP, the driver retrieves the vehicle and drives it out of the entrapment area where any passengers can rejoin the vehicle after they successfully pass through the ECP.

If a security violation is found, the sentry alerts ECP guards who initiate the security violation protocol; no further persons/vehicles are processed in or out until the security violation protocol has been completed. As previously stated, the security violation protocol is outside the scope of this project.

C. PRELIMINARY DESIGN

The team performed a Functional Analysis and derived a Functional architecture to begin Preliminary Design. These were modeled using Vitech's CORE, in order to ensure that system requirements and functions are properly aligned. This ensures traceability between requirements and functional architecture. This allowed the team to determine if there are any requirements that have been overlooked, or if there is any redundancy in the functional architecture.

The functional Architecture was then modeled using Operational, System, and Capabilities Views hierarchies expressed in Integrated Definition modeling (IDEF) and Enhanced Functional Flow Block Diagrams (EFFBD).

1. Preliminary Design Methodology

The ARAECS Team adopted an integrated architecture and modeling methodology, tied to defined requirements and measured through a weighted OMOE. The process to execute this methodology can be summarized as:

- Identify the required processes to accomplish the assigned mission.
- Allocate functions to the required processes.
- Allocate objects to the required functions.

2. Tools and Processes

The team selected CORE as the architecting software and ExtendSim8 as the modeling software. The principal criterion was the team's familiarity with both software packages and relative unfamiliarity with competing products. The team utilized CORE Version 8 for initial architecture input and transitioned the final project to CORE Version 9 for reasons of compatibility. Additional tools to assist in data management and analysis included Microsoft Excel and Minitab.

The results of the requirements and functional analysis were decomposed within the CORE database as the initial operational architecture. The principal operational functions were then modeled within the ExtendSim8 program as a discrete event simulator. Excel was used as a data handler that both fed the ExtendSim8 model and held the resultant data. Factor values, configuration of model variants, and responses were examples of values held within Excel. The team utilized Minitab to provide the Design of Experiments configurations and ultimately to conduct the statistical analysis of the model's responses.

a. Phase 1: Identify Required Processes

This phase began with the identification of discrete higher level requirements and the operational organization of the nominal agency tasked with conducting security functions at a Naval Restricted Area. These artifacts were used to build the baseline operational architecture which included:

- An overall, operational view of the conceptual solution
- A view of the security force organization
- A view that decomposed required security processes
- A view that denoted information flow between operational nodes with named need-lines

b. Phase 2: Allocate Processes to Functions

The second phase represents the first formal link between a performance model and the architecture model. The work required to prepare and measure the suitability of functions within the performance model was completed in this phase.

This phase began with the initial operational architecture. Modeling assumptions and constructs were developed that reflected the operational architecture and were then built within the performance model (ExtendSim8). From this, the initial performance model was baselined with representative data. Model factors that influence performance were identified, and then binned according to these four categories:

- Uncontrollable factors (noise)
- Physical improvements, such as those that would require military construction
- Technology improvements
- Human-based CONOPS improvements

Two Measures of Performance (MOP) were recorded from the models, and then combined into a single response value: Personnel Wait Time and Number of Security Violations. A single response was developed for the model so that a Design of Experiments (DOE) technique could be used to track performance-related factor variance. This single response, or OMOE, was derived from surveys from input and assistance of the two primary end user stakeholders: a manager with production responsibilities and a manager with security responsibilities. More information is provided in the OMOE development section on how the specific response was evaluated.

DOE was used to compare the baseline against changes in all factors with the exception of system noise factors. Statistical techniques were used to screen the factors that significantly influence overall performance. Additionally, the process examined DOE outcomes that only considered specific factors grouped according to the binning described earlier. This was meant to support the project's overall goal of extensibility to many environments that may not have ready resources to implement solutions based on resource constraints (e.g., insufficient funding for physical improvements). An overall "Super" version of the model was also assessed to provide a comparable end-point to the results of intermediate factors in the overall analysis.

The results of all factor variances were calculated. From these results a conceptual solution was identified based upon factor performance values.

c. Phase 3: Allocate Functions to System Objects

This phase began with the identification of the conceptual solution. Based upon technology research, representative technologies were identified that could reasonably achieve the performance model factors that correlated to them. The performance model was modified to accommodate a realistic interaction required based upon identified factor values, and an overall series of validation runs produced results for system comparison.

Initial cost estimation was done utilizing a back-of-the-envelope cost model to build a cost effectiveness curve. The most cost effective system solution was utilized for system architecture development.

The team returned to CORE and modified the operational architecture based on the above, and then developed the system architecture. The views included in the system architecture included:

- A view of system objects and their hierarchy
- A view of system functions and their hierarchy
- An allocation of system objects and system functions with the associated views

3. Performance Modeling Details ExtendSim8

The overall process of entry and circulation control of a restricted area follows the basic precepts of a client-server model. Clients, or personnel attempting to enter a restricted area, approach the entry point at random intervals. The ARAECS system is the server that executes the required system functions in processing their entry. ExtendSim8's built-in functions are able to closely emulate the principal ARAECS functions of entry and circulation control and report measures of performance.

4. Principal Security Aspects

As derived from higher-level requirements documents, there are four principal security protocols that the ARAECS system must be able to accomplish, illustrated in Figure 4:

- Validate badge and person
- Validate area authorities
- Screen for contraband
- Detect Duress

Validate badge and person. Each person that attempts entry into the restricted area must have a unique badge with corresponding picture identification. The badge must be valid (e.g., non-expired) and the person's identifying features must match the picture on the badge. ARAECS must ensure that only personnel with valid badges with a corresponding picture are admitted to a restricted area. Figure 4 shows the system function and corresponding modeling function.

Validate area authorities. Each person must be authorized access to the specific restricted area. The approval and enrollment process is outside the ARAECS system boundary and will vary depending upon the restricted area. ARAECS must only allow authorized individuals access into the restricted area. Figure 4 shows the system function and corresponding modeling function.

Screen for contraband. Each restricted area may have varying types of items that are prohibited. Basic examples of prohibited items include weapons, ammunition, explosives, illegal drugs, uncertified electronic equipment, and flame-producing items. Specific contraband restrictions vary depending upon the security level of the restricted area and risk assessments performed based upon the volatility of material inside the restricted area, e.g., explosives or special nuclear material. ARAECS must detect contraband prior to its introduction within the security area. Figure 4 shows the system function and corresponding modeling function.

Detect duress. Duress is defined as an individual who is compelled by force to willfully violate security requirements. Duress is a method that a potential adversary may use to leverage a person with valid badging and access to perform unauthorized acts within a restricted area. ARAECS must not allow personnel under duress to enter the restricted area. Figure 4 shows the system function and corresponding modeling function.

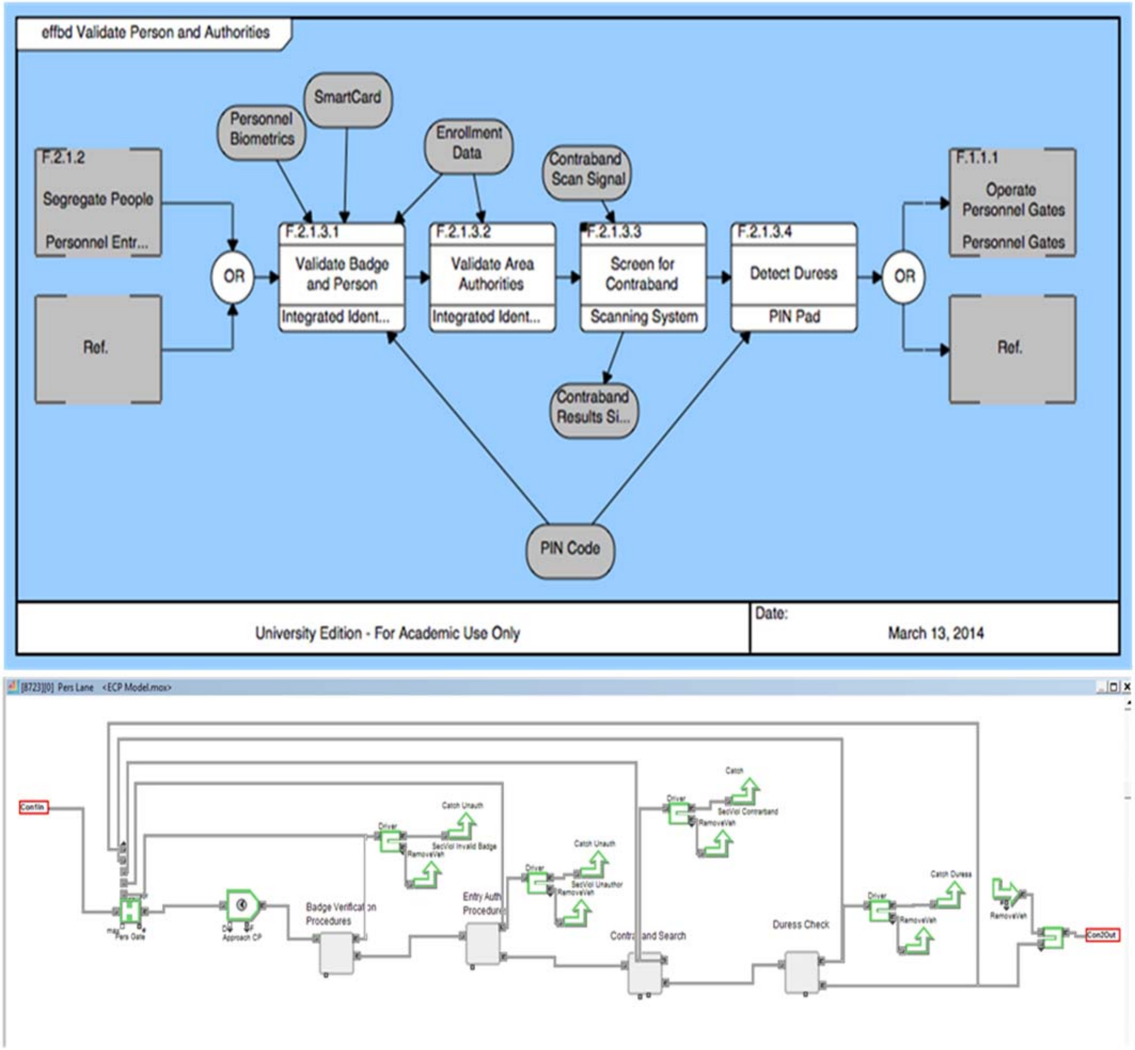


Figure 4. Principal security protocols, modeling capabilities mapped to system functions

5. Extended System Aspects

In addition to the four principal protocols described above, ARAECS, as represented in the performance model, must satisfy additional criteria:

- The ARAECS must perform its functions while accommodating a reasonable number of personnel into the server. This was modeled through the arrival times and distributions that represents a two-shift workforce across a twenty-four hour period.
- The ARAECS must also accommodate the introduction of vehicles into the restricted area while maintaining the four principal protocols.

- Security violators, as identified by the four principal protocols, must be removed from the system. Tactics, techniques, and procedures for security violation response are outside the system boundary of the ARAECS.
- ARAECS must be physically configured in a manner that supports the requirements. Examples of possible configuration changes include varying the number of entry points and the number of lanes that process personnel and vehicles. Per system requirements, ARAECS will segregate personnel and vehicles individually during processing.

6. Basic Model Construct

The model was constructed to allow the varying introduction of personnel and vehicles into queues to await individual entry to the restricted area. There was a single queue for vehicles awaiting entry, and a single queue for personnel awaiting entry. The personnel queue included drivers who entered a vehicle lane, prepared their vehicle, and then processed through the system as individuals. Upon successful personnel processing, drivers then rejoined their vehicles and entered the restricted area. Once personnel and vehicles entered the restricted area they remained for approximately eight hours, simulating a typical work shift, then returned to the entry point and processed out.

a. Arrival Times and Intervals

The quantity of personnel and shift lengths were roughly based upon the Trident Refit Facility at Naval Submarine Base Kings Bay, Georgia. The performance model addressed personnel arriving upon the following schedule:

- Random personnel entries not tied to a specific shift—this followed an exponential distribution with a mean of 1728 seconds (28.8 minutes).
- 1,500 personnel with Shift 1 scheduled to arrive at 0600 with a normal arrival distribution with a mean at 0600 and a standard deviation of 450 seconds (7.5 minutes).

- 1,500 personnel with Shift 2 scheduled to arrive at 1400 with a normal arrival distribution with a mean at 1400 and a standard deviation of 450 seconds (7.5 minutes).

As ExtendSim8 operates as a discrete event simulation within a client-server model, the team utilized entity creation blocks and distribution delays to recreate the schedule within the model, and is shown in Figure 5.

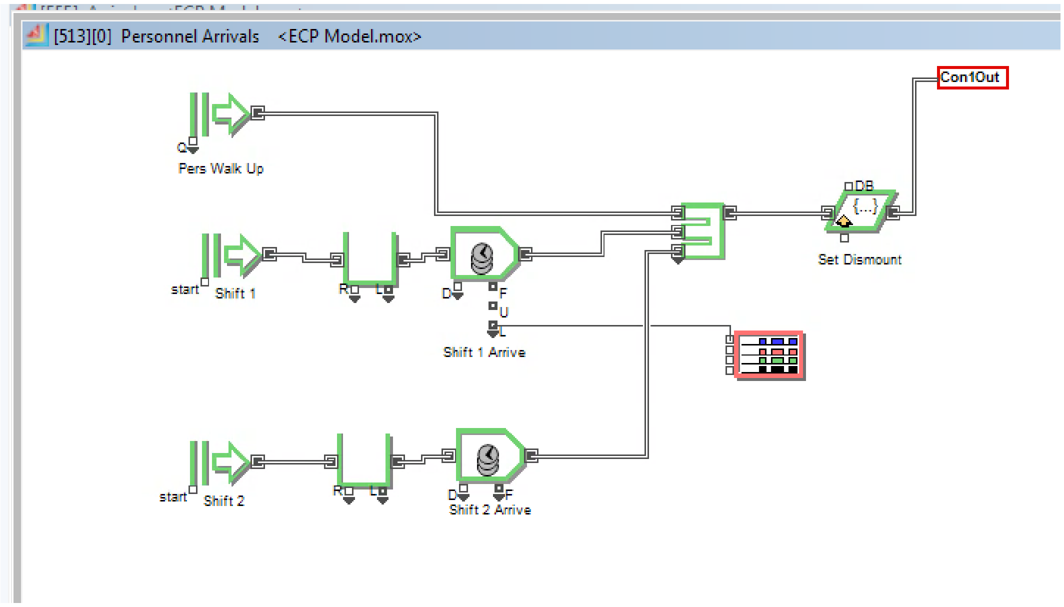


Figure 5. Method of modeling personnel arrivals

Restricted areas typically limit entry to select government vehicles. Vehicle arrival was modeled with the following schedule:

- Random vehicle entries not tied to a specific shift - this followed an exponential distribution with a mean of 2468 seconds (41.13 minutes).
- A morning rush period of vehicles—this followed an exponential distribution with a mean of 450 seconds (7.5 minutes).
- An afternoon rush period of vehicles—this followed an exponential distribution with a mean of 1023 seconds (17.1 minutes).

As with personnel arrivals, the team modeled the schedule within ExtendSim8 utilizing entity creation blocks and stochastic delays as demonstrated in Figure 6.

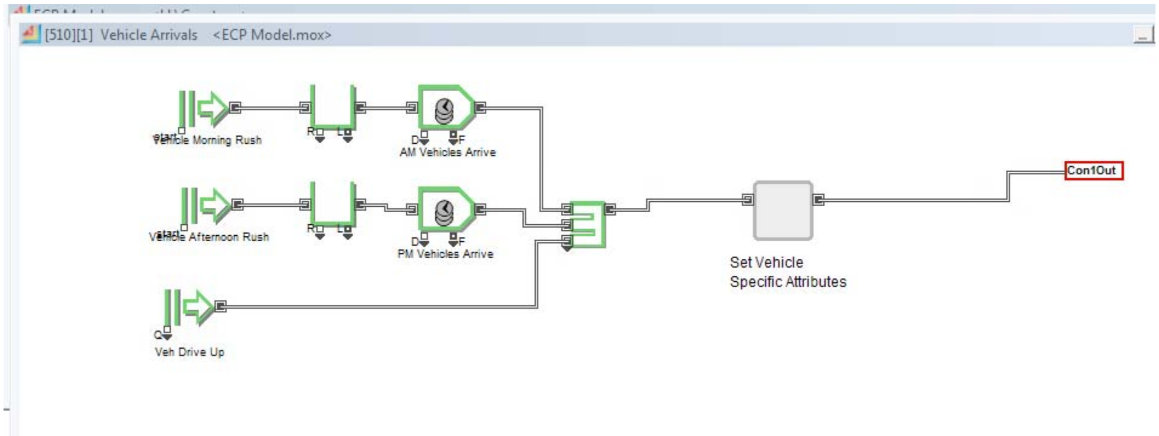


Figure 6. Method of modeling vehicle arrivals

Shift work time, which delayed individuals who were authorized entry until they attempted exit, was based upon a normal distribution with a mean of 28,800 seconds (8 hours) and a standard deviation of 900 seconds (15 minutes).

b. Entry Control Points

The model accommodated five entry control points (ECP). The number of ECPs that were active in any of the system configurations was a system factor that could be varied. Each ECP had the same type and number of processing lanes. For both vehicle and personnel lanes, there were three types:

- Dedicated entry lanes
- Hybrid lanes that processed personnel/vehicles for entry or exit
- Dedicated exit lanes

The team modeled the maximum plausible number of entry control points within ExtendSim8 and then piped entities through those blocks within the context shown in Figure 7. As different variants utilized differing numbers of ECPs, the factor value of active ECPs activated the correct number of entry points. Inactive ECPs were blocked.

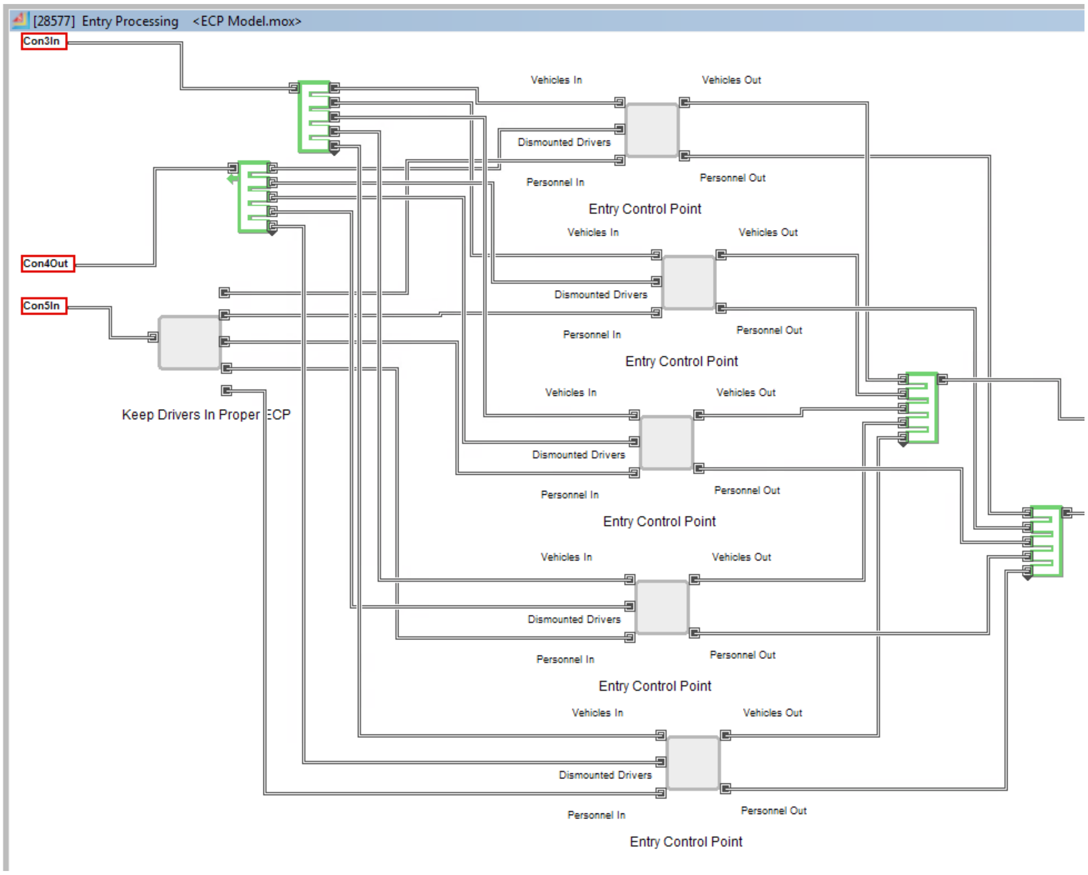


Figure 7. Method of modeling physical nature of ECPs

The model accommodated a maximum of five lanes of each type for both personnel and vehicles. As with the ECPs, the actual number of active lanes was an adjustable factor in the model. Table 4 provides a summary that compares the number of active ECPs in the baseline compared to the Physical Variant.

Factor	**Type**	**Baseline Value**	**Physical Variant Value**
Number of ECPs	Physical	3	4
Dedicated Vehicle Entry Lanes	Physical	0	0
Veh Entry/Exit Lanes	Physical	2	4
Dedicated Vehicle Exit Lanes	Physical	0	0
Dedicated Personnel Entry Lanes	Physical	1	5
Dedicated Personnel Exit Lanes	Physical	5	5
Personnel Entry/Exit Lanes	Physical	1	5

Table 4. Values for Physical Modeling Factors of ARAECS

c. Technology Factors

Technology factors were largely related to effectiveness probabilities and delay times related to the four principal system protocols. Additional factors related to the contraband search functions. Based upon the system architecture, there are three types of searches:

- Cursory Personnel Search. The cursory search is a quick visual assessment required of all personnel requesting entry into the restricted area.
- Detailed Personnel Search. The detailed search is required for all personnel requiring escort and, according to the requirements and the architecture, for randomly selected personnel.
- Vehicle Search. A different factor was used for vehicle searches since fundamentally different techniques and technologies are utilized for vehicle searches. All vehicle searches are considered detailed searches.

Table 5 summarizes the differences in the technology-related factor values between the baseline model and the Technology Variant

Factor	Type	Baseline Value	Tech Variant Value
Probability of Detection (Pd) for detailed search	Technology	0.85	0.95
Pd for cursory search	Technology	0.01	0.01
Delay detailed search (s)	Technology	120	30
Delay Cursory Search (s)	Technology	0.1	0.1
Delay badge validation (s)	Technology	4	1
Delay authorization validation (s)	Technology	10	10
Delay duress check (s)	Technology	3	1
Pd for unauthorized badge	Technology	0.9	0.99
Pd for unauthorized access	Technology	0.9	0.99
Delay for Vehicle Search (s)	Technology	240	240
Pd for Duress Check	Technology	0.99	0.99
Pd for Vehicle Contraband	Technology	0.4	0.4

Table 5. Values for Technology Modeling Factors of ARAECS

d. CONOPS Factors

CONOPS factors address the rates at which the guard force personnel utilize cursory and detailed searches. This factor category was meant to address techniques to increase overall system effectiveness without a need for significant resources (e.g., construction of additional control points, investment in new technologies, etc.). However, in most cases implementing the CONOPS category of improvements would require additional manpower, which could be a significant cost. There are three CONOPS factors in two sub-categories:

- Rate of detailed search for entry/exit. The detailed search is the segment of personnel requesting entry or exit that are sent to a detailed search conducted by the entry control personnel. The use of a different rate for entry and exit allows the model to show different results based upon a greater acceptance of risk.

- Rate of random check. The random check is provided by an additional security unit that provides detailed searches at an unpredictable schedule, such as one hour out of every eight.

Table 6 summarizes the differing values for CONOPS-related factors in the baseline model and the CONOPS Variant.

Factor	Type	Baseline Value	CONOPS Variant
Rate of Detailed Search	CONOPS	0.5	1.0
Rate of Detailed Search Exit	CONOPS	0	0
Rate of Random Check	CONOPS	0.15	0.15

Table 6. Values for CONOPS Modeling Factors of ARAECS

e. Noise Factors

The ARAECS model was built to accommodate uncontrollable factors (noise values) for a robustness sensitivity test. The following values are not based upon historical numbers but on subject matter expertise from security professionals. The noise factor values remained the same for all variants and were only adjusted in a final sensitivity study, summarized in Table 7.

Noise Factor	Value
Rate of invalid badges	0.01
Rate of unauthorized personnel	0.005
Rate of contraband	0.05
Rate of duress	0.0001
Rate of Personnel Requiring Escort	0.1
Rate of vehicle contraband	0.01

Table 7. Values for Noise Modeling Factors of ARAECS

f. Baseline Values and Modeling Insights

The team analyzed the ExtendSim8 model for ARAECS with baseline values with the initial values indicated in Tables 4–7 and collected data for 100 runs. The baseline factor values did not represent an existing location, but approximated a general naval industrial facility that is reliant on a manpower-based physical infrastructure pre-dating the Global War on Terror.

Based upon the 100 runs of the baseline variant, the average vehicle wait was only 456 seconds (7.6 minutes) but the average personnel wait was about three hours. It is important to note that clearly no existing system requires a three-hour wait time—this is just a baseline value in the modeling to compare with the variants discussed later. The system processed 5,154 security entries/exits each day with an average of 118 security violations.

D. OVERALL MEASURE OF EFFECTIVENESS (OMOE)

The ARAECS model produced two measures of performance considered important in the customer ranking. The first was delay time while waiting to process through the ECP. The second was the number of security violators improperly processed. The customer stakeholder inputs indicated that lowering the number of security violations is more important than a shorter wait time. This is not surprising—security professionals know that even one improperly admitted person can lead to disastrous consequences. Of course, in reality there are different “levels” of security violations. A misspelling on a badge is not the same as an individual intentionally smuggling in plastic explosives. However, the team decided that for the purposes of this model, all security violations would be treated the same. Further research may be able to better quantify the severity of the various security violations and thus “fine-tune” the OMOE.

Due to the scale issues between delay times in the tens of thousands of seconds and a relatively few number of security violations, a simple summation of measures of performance (MOPs) could mask variations. Therefore, the team decided on a logarithmic weighting value within a multiplicative OMOE.

The second challenge of the OMOE was related to the overall system goal to minimize wait time. In some cases the DOE showed wait times at or near zero. Therefore, the developed OMOE took a fractional approach using a value of 5000 seconds, which was selected because it is approximately halfway between the baseline wait time of 10,656 seconds and zero. In the OMOE, a wait time of zero makes the wait time factor 1.0.

Full derivation of the OMOE can be found in Appendix B of this report. Mathematically, the OMOE is:

$$OMOE = \frac{(5000 + w_t)}{5000} n_{sec}^{1.7}$$

1. Design of Experiments (DOE) Methodology

As one of the project goals is to produce an extensible design for varying configurations of plausible entry control systems across the Navy, this DOE conducted analyses on four inter-related security designs: (a) a full system analysis that accommodated all 22 design factors; (b) an analysis of the system constrained to technology factors; (c) an analysis of the system constrained to physical factors; and, (d) an analysis of the system constrained to CONOPS factors. Factors that may not have screened within the full system analysis were still considered in the constrained follow-on analysis. The reason this was done was because organizational budgets and existing infrastructure may not support all aspects of the system solution. One command may not have military construction funding required to upgrade physical entry lanes or manpower sufficient to employ some of the CONOPS solutions, but they may have OPN procurement dollars to support technology investment. Likewise, another command may have existing infrastructure with multiple entry control points, but need to make informed decisions on how to best upgrade the legacy structures. The interrelated nature of the DOE was intended to address these local issues. The team conducted all DOE and statistical analysis with the Minitab16 software suite.

a. Full System Screening Within the Design of Experiments

The Full System Screening DOE looked at a Resolution III Plackett-Burman design made of 22 factors and two levels, three replicates and 144 total runs. The risk of running a Resolution III design is that confounding factors are not easily identified, so potential future work could utilize a different experimental design utilizing the same basic ExtendSim model in order to provide additional insight within factor interaction. Using the OMOE as a response, eleven of the original twenty-two factors could be discarded as having a lesser impact on overall system performance. These are denoted in Figure 8.

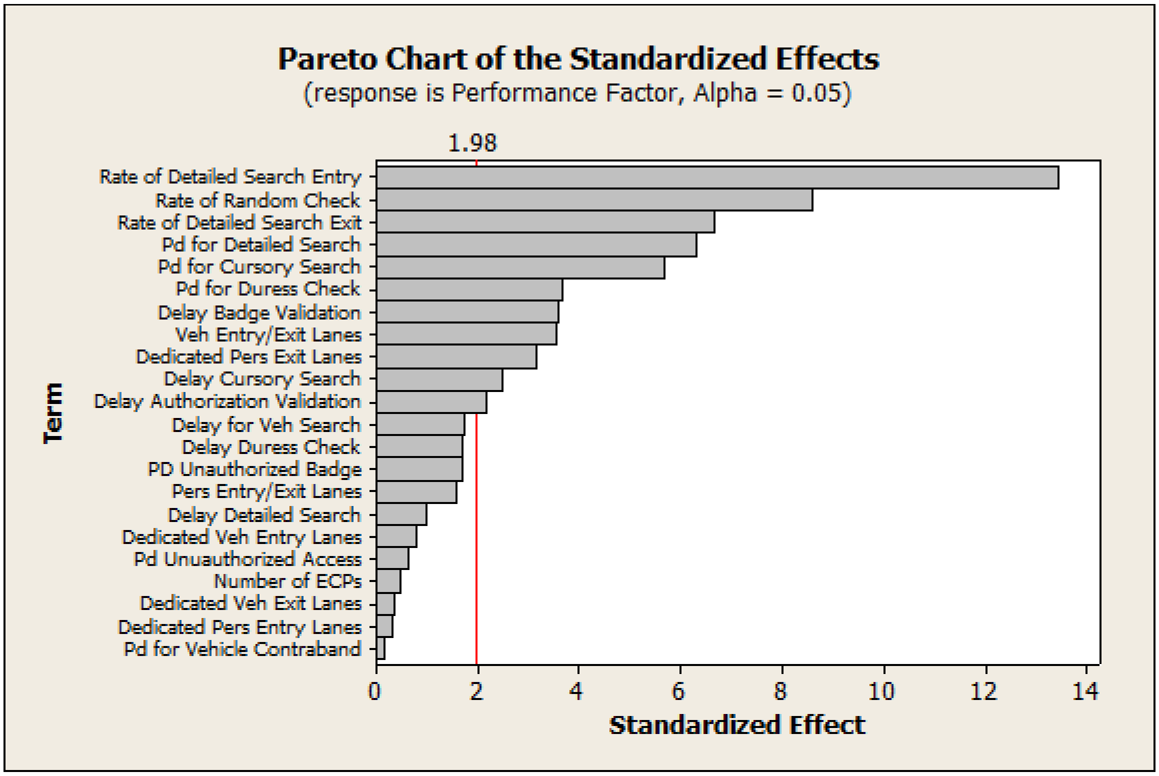


Figure 8. Original Factors Within the Design of Experiments

The top eleven factors, each with two levels, were then re-analyzed under a new Resolution IV Factorial Design for three replicates of 128 runs (total of 384 runs). The benefit of reducing the factors existed in employing a Resolution IV design that can provide greater insight into two-factor interactions (with a continued issue that these may in turn be affected by interactions with other factors).

The top two factors that screened in the DOE involved the rate of detailed search for personnel entry and the rate of random personnel checks. The detailed search is a more effective search, thus more detailed searches result in fewer security violations. Increasing the rate of random checks provides essentially the same result, so while these two factors screened at the top, they ultimately demonstrate very similar capabilities of the system. Figure 9 graphically depicts the standardized effect of each factor on the response. The red line in Figure 9 is the statistically significant threshold for an alpha value of 0.05, thus the analysis considered any factor value exceeding the threshold as having impact on the OMOE.

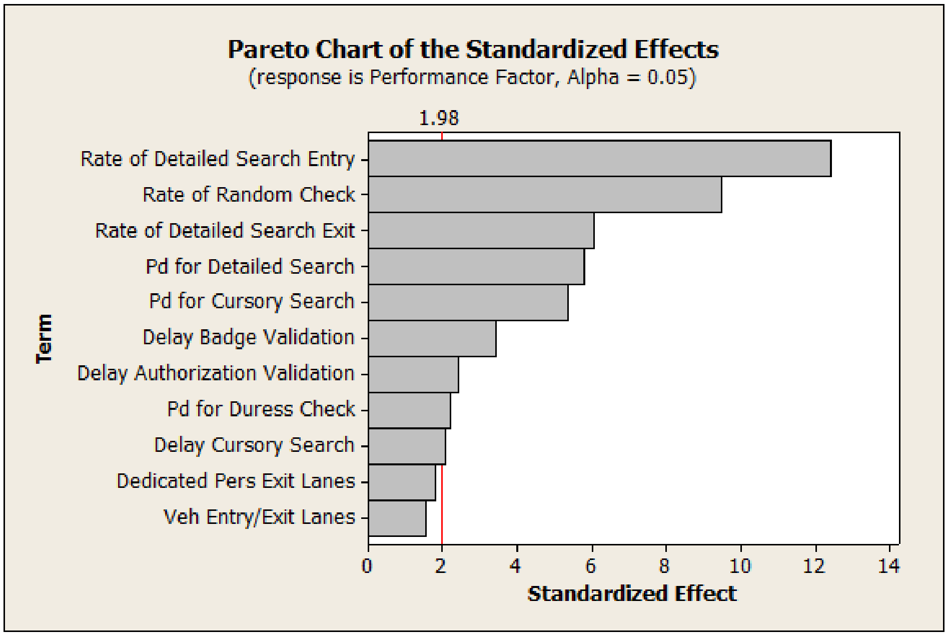


Figure 9. Screened Factors Within the Design of Experiments

The factors that did not screen did include some surprises, such as adding additional lanes to process personnel quickly. One might think that adding additional lanes would significantly reduce wait times—improving the OMOE. However, without adding in additional capability to detect security violators, faster throughput allows a greater number of security violators to enter, which in turn negatively affects the OMOE, which is more heavily weighted towards reducing security violators. Other examples of this effect included decreasing the delay time for badge validation and delay for authorization validation. These insights are graphically depicted in Figure 9. The x-axis value in Figure 10 depicts factor values and the y-axis is the analyzed response. Since a lower response value indicates a "better" outcome, the team focused on those factors that achieved the lowest OMOE values.

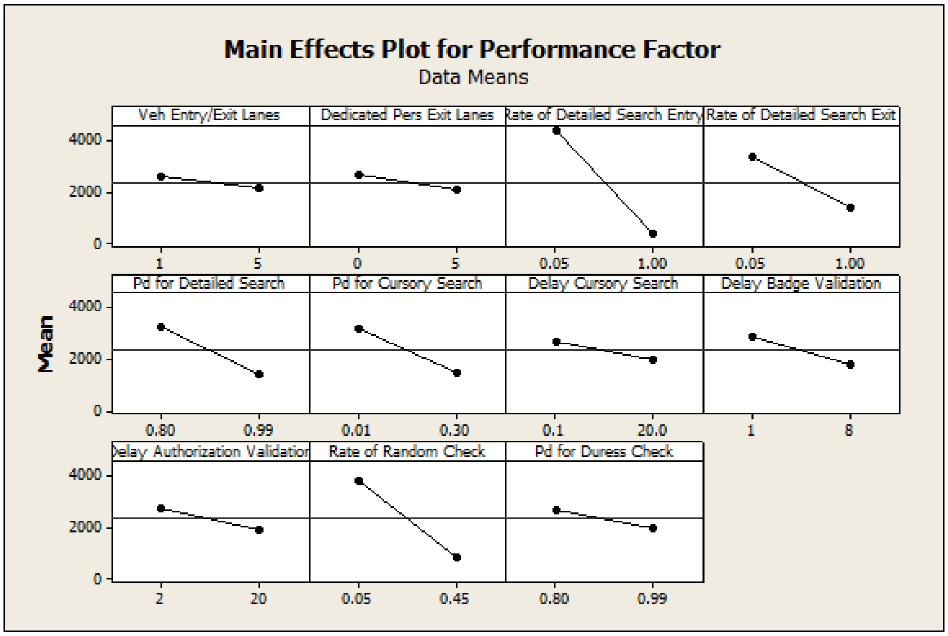


Figure 10. Main Effects Plot for Screened Factors Considering the OMOE

b. Interaction Plot for the Performance Factor

The team conducted an analysis between the interactions of various factors, depicted in Figure 11. In this graph, the response is mapped between two factors, with a lower response value indicating a “better” response. As in the previous plots, the team judged factors where the OMOE did not appreciably change as less important and instead focused on higher payoff investments that resulted in better OMOE respones.

Utilizing the Level IV resolution of the post-screened DOE as the source of the interaction plots is a valid method to determine the interactions between two factors. The most notable interaction included changing the rates of detailed search and performing a random check. These two actions, measured independently in the model, perform the same functional task. Maximizing one of these two factors provides no additional benefit when changing the second factor. Therefore, the “random check” factor was eliminated from further designs with the full capability associated into the rate of random check.

Figure 11 suggests that additional interactions could be in play, however, since further analyses focused on constrained physical, technology, and CONOPS factors, overall interaction analysis is limited in this report. Future work for specific locations could build on this report’s interaction analysis, reduce the number of factors to those relevant to the local condition, and increase the resolution to a Resolution V/VI experiment, and better estimate the effects of two and three factor interactions.

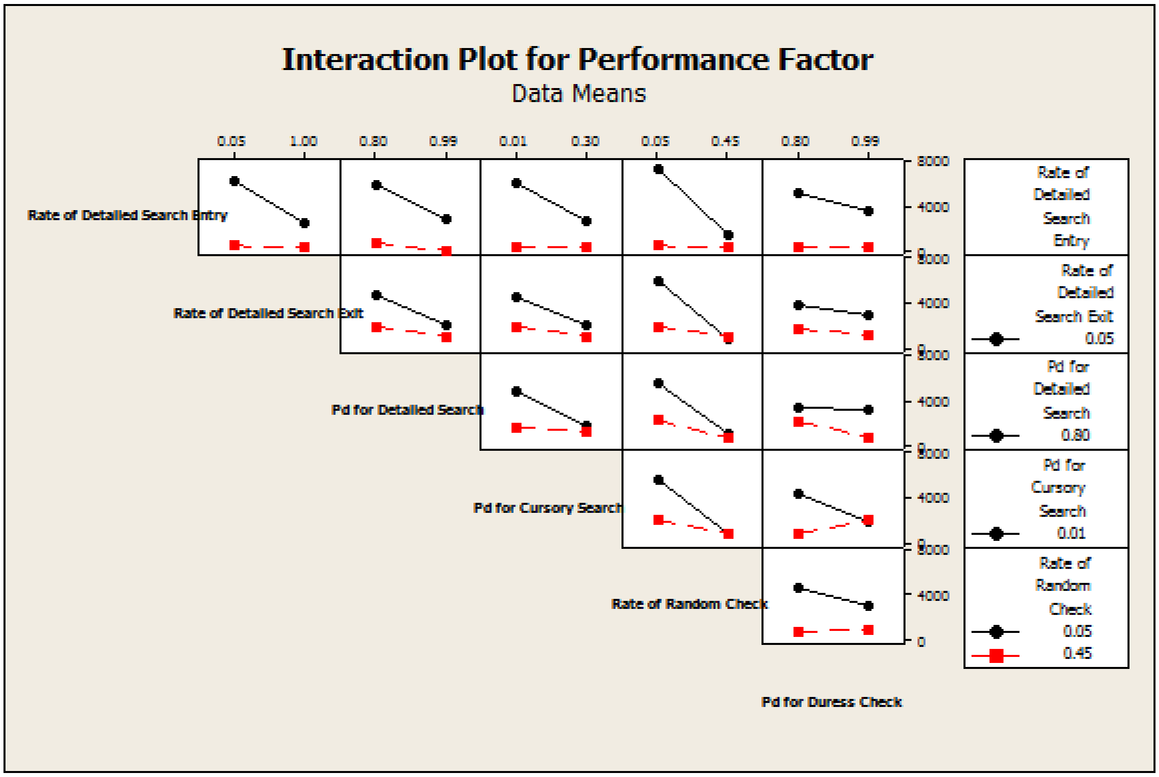


Figure 11. Interaction Plot for Screened Performance Factors

c. *Additional DOE Constrained to Either CONOPS or Physical*

Due to the fact that the ARAECS project is intended to be extensible to a diverse group of Navy locations, analyzing responses when the factor variance was constrained to either CONOPS or Physical provided insights for organizations constrained with respect to particular resources. In some cases, a command may have the capability to put additional guards on station for increased checks, but may not have access to timely MILCON dollars to effect physical improvements. In other cases, technology may not truly become mature, or the command may lack the data-based network resources to execute a full technology option. In these circumstances, the command may examine opening additional gates or investing in MILCON until technology matures. In constraining the view of each of these sub-analyses, the number of levels was increased to identify non-linear behavior and breakpoints.

As a secondary reason to examine physical CONOPS, the team was interested in lowering the wait time as much as possible. While both customer surveys indicated that precision of the search had the top priority compared to speed of search, the reality in contemporary Navy industrial facilities is that they employ large numbers of unionized civilian and contractor employees. Wait time must always be a consideration because the costs associated with unproductive wait time are a huge concern, not to mention the impact on industrial facility production and schedule.

CONOPS is generally (although erroneously) regarded as a relatively low-cost solution, and can be a favored option for something implemented quickly and within an existing organizational structure. With respect to this reality, the team examined a greater number of levels within the CONOPS factors to determine if there was a non-linear relationship with respect to potential CONOPS improvements. The new experiment utilized a three factor, five-level, full-factorial design. The possible additional insights that might be gained from utilizing more levels were considered worth the additional computer processing time. However, even with the additional levels, the main effects plot solely considering CONOPS demonstrated a fairly linear relationship without breakpoints, as graphically depicted in Figure 12.

Additional results from the CONOPS analysis included the finding that all main factor effects and two factor interactions screened as statistically significant (alpha = 0.05). The similar confounding factors between the random check and detailed search were evident in this constrained analysis as it was in the full system.

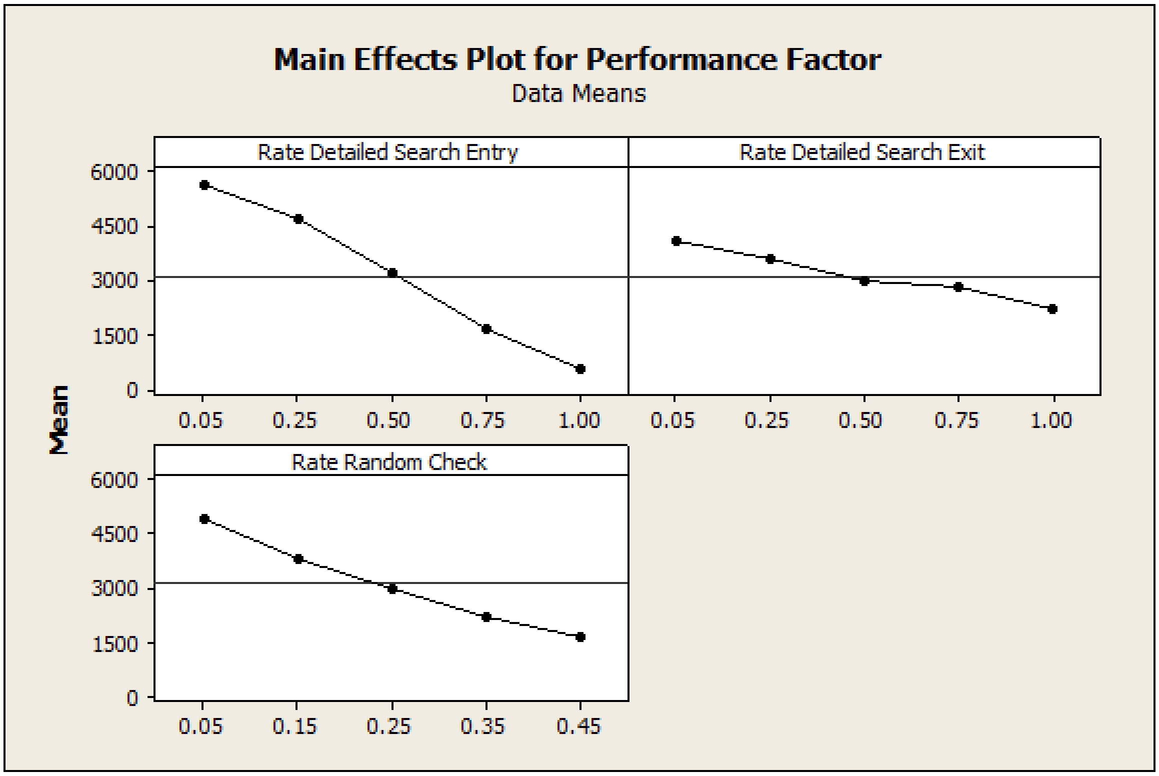


Figure 12. Main Effects Plot Constrained to CONOPS Factors

The physical analysis had seven factors with three levels within a full factorial design. Dedicated vehicle lanes, and personnel exit lanes did not screen, but the number of ECPs and entry lanes did. The results are graphically summarized in Figure 13. Changing the number of vehicle lanes had virtually no impact on the response. The team judged that this was largely due to the orders of magnitude difference in the number of vehicle drivers (tens to hundreds) compared to dismounted personnel at the gate (thousands). Personnel exit lanes had minimal impact of response but entry lanes (to include those hybrid lanes that allow entry or exit) did. There was a small breakpoint in this analysis that showed that increasing the number of ECPs to four and three dedicated personnel lanes could provide better a better return on investment than simply selecting the maximum value (five).

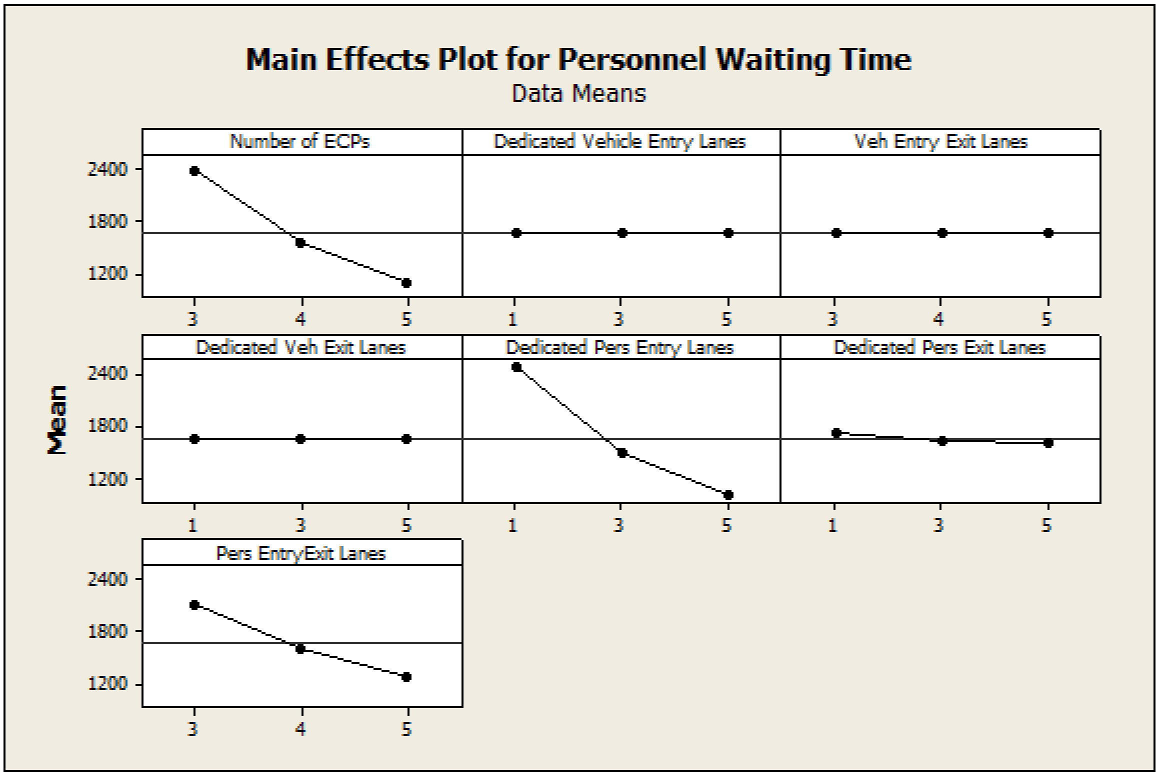


Figure 13. Main Effects Plot Constrained to Physical Factors Considering Wait Time.

2. Summary of Insights and Results of the Initial Variants

In addition to the DOE factor analysis of physical and CONOPS, four initial variants were constructed based upon improving factors within the CONOPS, Technology, and Physical groupings that utilized static factor values based upon reasonable values. The OMOE computation remained the same as the DOE. An additional variant was constructed that utilized the best values from each of the three capability-type variants, which was known as the “Super.” The Super was analyzed as a comparison and end-point, i.e., a “best-case” OMOE.

As expected, the Super Variant outperformed all others with the lowest wait times and security violations. By OMOE, the next best performer was the CONOPS variant. The technology and physical variants had similar OMOEs. While the CONOPS variant had a relatively acceptable OMOE, this was due to the small number of security violators that penetrated the access point. The average personnel wait time was approximately five hours, which actually was a 68% decrease in wait time performance compared to the Baseline variant.

The Technology and Physical variants both had average wait times less than an hour, at the cost of a high number of security violators. Stakeholder input, however, prioritized system accuracy, i.e., detecting security violators, over the speed of the system. Thus, it would not likely be acceptable to the stakeholders to invest in a new entry system without at least an improvement in catching more security violators.

This leads us to the following two significant insights:

- A workable solution must integrate aspects of CONOPS, technology, and physical improvements.
- Without an integrated design, a system might achieve few violations or short waiting time, but not both.

Table 8 is a summary of the MOPs and OMOE between all the variants. Of note in this table is that the MOP values varied significantly between the Technology and Physical variants but produce a relatively similar value.

	BL	**CONOPS**	**Technology**	**Physical**	**Super Option**
Average Vehicle Wait (s)	456	480	443	9	12
Average Personnel Wait (s)	10656	17907	2810	745	93
Security Violations	118	32	108	137	20
OMOE	10387	1640	4452	4926	170

Table 8. Summary of Modeling Results Based on the Initial Variants

a. Development of Alternative Variants

As none of the initial variants adequately addressed the MOPs, the ARAECS Team revisited the DOE insights for an alternative solution that performed as well as the "Super Variant," but without maximizing all performance factors to achieve the desired responses for both precision and speed. The seed-capability for this improvement is in the detailed search factor. Contraband is the most common form of security violation. As discussed earlier, all contraband is treated the same in the model—whether plastic explosives or an unauthorized flash drive. Further research may be able to provide more insight by "weighting" contraband differently based on an assessment of the threat it represents. Detailed searches give the best results for eliminating contraband but also take the most amount of time. ARAECS' first five variants apply the detailed search function randomly. The team pondered the question: Is there a way to select individuals for detailed searches smartly?

Empirically, if an individual was known to be trustworthy based on some standard criteria, this person could be designated as "pre-screened" and allowed to skip the random search. Others without this "pedigree" could be given random searches at a higher rate. The team picked the DOD security clearance process as an institutionalized system that allows a security force to compare relative trustworthiness as a result of background checks and command monitoring. In other words, the practice of holding a security clearance establishes a baseline of trustworthiness. Cleared personnel understand that certain violations put their clearance at risk and generally do not engage in those activities. However, as recent experience has shown, there is no absolute guarantee of trustworthiness—thus even cleared personnel require some random checks.

b. "Hybrid" Variant-based Approaches

Utilizing the security clearance process, the hybrid ARAECS variant assumes that 40% of the typical workforce that enters the restricted area possesses at least a SECRET (National Agency Check with Local Agency Check (NAC-LC)-based) clearance. In actuality, this may be an increase in the proportion of cleared personnel in a waterfront industrial area, and therefore its cost must be considered. Personnel possessing a clearance are allowed to process through a separate ECP where they are given a passing visual search for gross contraband violations (e.g., visible weapons). As discussed earlier, since there are no absolute guarantees, 5% of cleared personnel are still selected for random detailed screening.

In the physical category, two additional, dedicated personnel entry lanes were added for a total of 3, as an insight from the DOE.

In the technology category, the effectiveness of the detailed search was raised from 0.85 to 0.95. As in the hybrid design, fewer detailed searches must be conducted with this higher confidence of success. Additionally, an integrated system of rapid and precise screening was envisioned that seeks human capital efficiencies and removes human error. The conceptual suggestion for such a system includes an integrated smartcard, PIN, and biometric system.

Ultimately, three hybrid variants were assessed and are summarized in Table 9. The differences between them deal with flow patterns dependent upon differing physical aspects or dynamic lane openings, and are summarized in Table 9.

Hybrid-based Variant Approaches	**Dedicated Personnel Entry Lanes**	**ECPs**	**Additional Notes**
Hybrid - A	1	4 (including one dedicated to prescreened personnel)	
Hybrid - B	3	4 (including one dedicated to prescreened personnel)	Opens five additional lanes at each ECP during rush periods
Hybrid - C	3	5 (including one dedicated to prescreened personnel)	Opens five additional lanes at each ECP during rush periods

Table 9. Description of Hybrid Variants

c. Hybrid-based Variants Results

Based on our OMOE, all hybrid variants outperform the Super variant. Once again, this result is due to the lowest numbers of security violations, relative to all other variants. Originally Hybrid-A was intended to stand alone, but because of its average wait time of over an hour, the team looked at additional options (Hybrids -B and -C) to reduce wait time. The numerical results of these Hybrid variants are summarized in Table 10.

	BL	Super	Hybrid-A	Hybrid-B	Hybrid-C
Average Vehicle Wait (s)	456	12	457	457	229
Average Personnel Wait	10656	93	4284	1649	1044
Security Violations	118	20	6	6	7
OMOE	10387	170	44	31	30

Table 10. Hybrid Variant Results Summary

3. OMOE Sensitivity

The selection of an appropriate exponential weighting factor is certainly subject to debate, but its foundation is in the customer indications of a preference for system accuracy (i.e., the fewest security violations possible) over system speed. The modeling team conducted a sensitivity analysis that removed the weighting factor and treated speed and security violations equally. Table 11 summarizes the values of the sensitivity analysis: the top four rows are a summary from the previously addressed analysis and the bottom row is the new OMOE computed from the same MOP values but using a non-weighted product. These competing OMOE values were used to build Table 12, which ranks the variants from best to worst utilizing both weighted and non-weighted techniques. The lists are virtually identical.

	Baseline	CONOPS	Technology	Physical	Super	Hybrid-B
Average Vehicle Wait (s)	456.26	479.51	443.04	9.50	11.59	457.49
Average Personnel Wait (s)	10656.16	17907.47	2810.34	745.43	92.75	1645.56
Security Violations	117.77	31.79	107.71	136.95	20.31	7.25
Original OMOE	10386.62	1640.22	4451.80	4926.16	170.25	38.56
Non-Weighted OMOE	368.77	145.65	168.25	157.37	20.69	9.64

Table 11. OMOE Sensitivity Results Summary

	Baseline	CONOPS	Technology	Physical	Super	Hybrid-B
Average Vehicle Wait (s)	456.26	479.51	443.04	9.50	11.59	457.49
Average Personnel Wait (s)	10656.16	17907.47	2810.34	745.43	92.75	1645.56
Security Violations	117.77	31.79	107.71	136.95	20.31	7.25
Original OMOE	10386.62	1640.22	4451.80	4926.16	170.25	38.56
Non-Weighted OMOE	368.77	145.65	168.25	157.37	20.69	9.64

Table 12. Parametric Ranking of Variant Through Differing OMOE Calculation

The results of the non-weighted sensitivity analysis indicate no change to the overall selection of the Hybrid-B and Super variants as being to top two performing configurations. There is a minor re-ordering between the Technology and Physical variants that does not affect the overall analysis. As a result, the weighted OMOE calculation is determined to be sufficient.

4. Robustness Sensitivity

The ARAECS model was designed to allow varying the uncontrollable factors so that a robustness sensitivity analysis could be conducted. Based upon back-of-the-envelope cost assumptions, Hybrid-B was the most cost-effective, and was the basis for the robustness analysis.

The primary intent of the robustness sensitivity analysis was to eliminate the question, “Did the selected security violator values have an effect on the system performance?” For all analysis conducted to this point, controllable factor values such as the number of entry lanes, performance of contraband scanners, or rate of random searches were treated as the signal. Uncontrollable factors, such as the rate of personnel carrying contraband or number of personnel requiring escort were treated as noise, and their selected values were kept constant. The robustness sensitivity utilized the Hybrid-B signal factors, since Hybrid-B was the most effective variant per OMOE, kept those signal factors constant, and then varied the values of the noise factors. The purpose of this analysis was to determine if the nominal design solution (Hybrid-B) could still adequately perform even if noise factors varied beyond the modeling assumptions. This sensitivity also demonstrated potential breaking points, a key factor in accomplishing the overall project’s goal of maintaining extensibility across the Department of the Navy to commands that may have conditions that do not precisely match the original analysis’ noise value assumptions.

Other than holding signal constant and varying noise, the model and OMOE computation remained precisely the same as the original variant analysis. The noise values were multiplied by factors of 1.25, 1.5, 2.0, and 5.0 in an attempt to find a breaking point. The robustness sensitivity analysis revealed that it takes violation and escort rates 5 times that of the original design assumptions for Hybrid-B to perform worse than the Super variant. Noise variances make minimal difference on the personnel wait time, even at the 5x factor.

Based upon the results of this robustness sensitivity analysis the team is confident in the robustness of the Hybrid-B construct and that even if any errors were made in selecting the noise factor values, the differences would not affect the overall system conceptual design.

Table 13 summarizes this analysis with the MOP and OMOE values. The Super column is utilized for comparison. Note that in Table 13, the OMOE value for the Hybrid-B does not exceed, i.e., perform worse, until the noise factors are increased by a factor of 5 (706 versus 170).

	Super	**Hybrid-B**	**Increase noise 1.25x**	**Increase noise 1.5x**	**Increase noise 2.0x**	**Increase noise 5.0x**
Average Vehicle Wait (s)	12	457	456	456	448	448
Average Personnel Wait (s)	93	1649	1666	1678	1729	1939
Security Violations	20	6	8	11	14	39
OMOE	170	31	47	74	114	706

Table 13. Parametric Analysis of OMOE Performance with Varying Noise Factors

E. SYSTEM ARCHITECTURE SUMMARY

1. Hybrid-B: High Level Operational Concept

The Hybrid-B Variant is an integrated entry control system that utilizes a combination of manpower, physical control features, and technology to control personnel, validate entry requirements, and screen for contraband. It physically interfaces with an existing boundary system (i.e., perimeter fence) and electronically interfaces with an enrollment database. As shown by the modeling discussed above, it is highly robust with respect to the rate of unauthorized entry and personnel requiring escort. Its defining feature is the pre-screening of personnel through the use of the DOD security clearance background checks in order to allocate the majority of detailed searches to personnel that are relatively unknown and thus represent a higher risk. Figure 14 is a pictorial representation of this system. The red line indicates the secure area boundary.

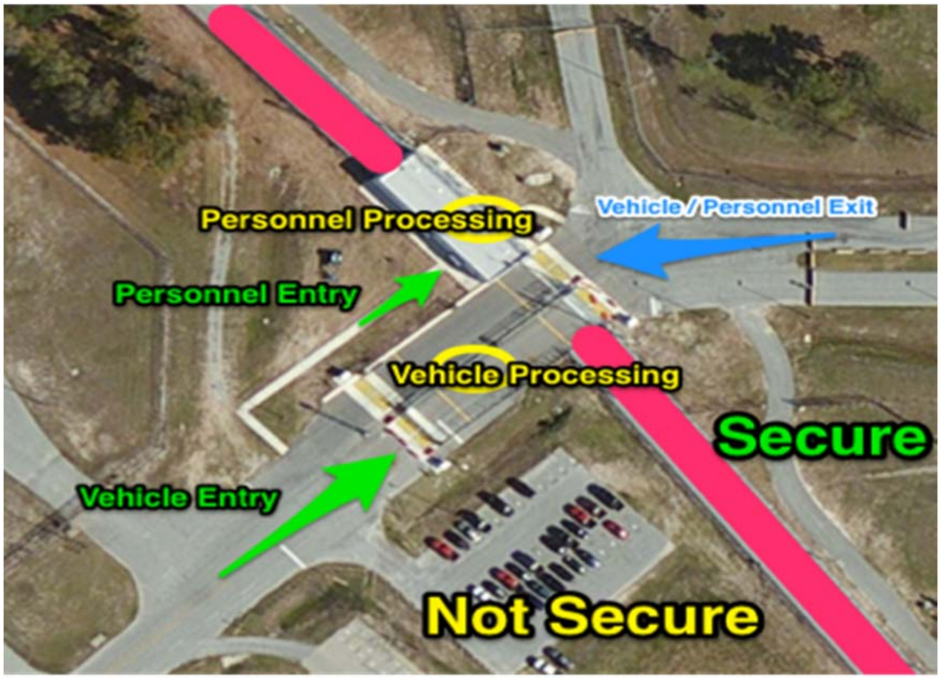


Figure 14. Overall Conceptual View of ARAECS

(1) Prime Directive. Entry control and processing supports security operations in a fully realized restricted area. Security for this type of area can be a System of Systems (SoS), or a System with very complex subsystems. The larger operational context that ARAECS supports is: Deny unauthorized access to critical naval assets.

Therefore, ARAECS, either as a complex subsystem, or a standalone system in a SoS approach, is designed to accomplish the prime directive to: Control authorized entry into restricted areas.

(2) Environment. The Hybrid-B is based upon a work area that handles approximately 3,000 people per day, evenly split between two shifts, and separated by an

average of eight hours spent within the restricted area before personnel egress. In addition to controlling personnel, the system is designed to handle the influx of several hundred vehicles a day with concentrated arrivals during the morning and afternoon rush periods.

(3) Pre-screening. The Hybrid-B modeling was based on 40% of the 3,000 workers having adjudicated security clearances equivalent to a SECRET NAC-LC. These personnel are processed through an expedited contraband check that only cursorily checks for gross abuses of contraband through a visual check. However, to maintain integrity of this trust-based screening, 5% of these individuals are randomly selected for a detailed screening. All other individuals are given a detailed contraband screening.

(4) Physical Nature of the Entry Control Point. The overall system is based upon one dedicated entry control point for the pre-screened personnel and three additional entry control points for all other personnel. Each entry control point has two vehicle lanes that can be used to screen vehicles on either entry or exit. For personnel, there are three lanes dedicated to entry, five lanes for dedicated exit, and three lanes that can be used for either personnel entry or exit. Each ECP has the capability to open five additional lanes for entry during the shift change periods.

(5) Technology Capability Measures of Performance. Rapid and accurate entry control is performed through an integrated computerized system based upon a smart identification card, a personal identification number that doubles as a covert duress indication system, and stored biometrics. It relies upon the “something you have, something you are” concept of secure entry control.

2. Use Cases

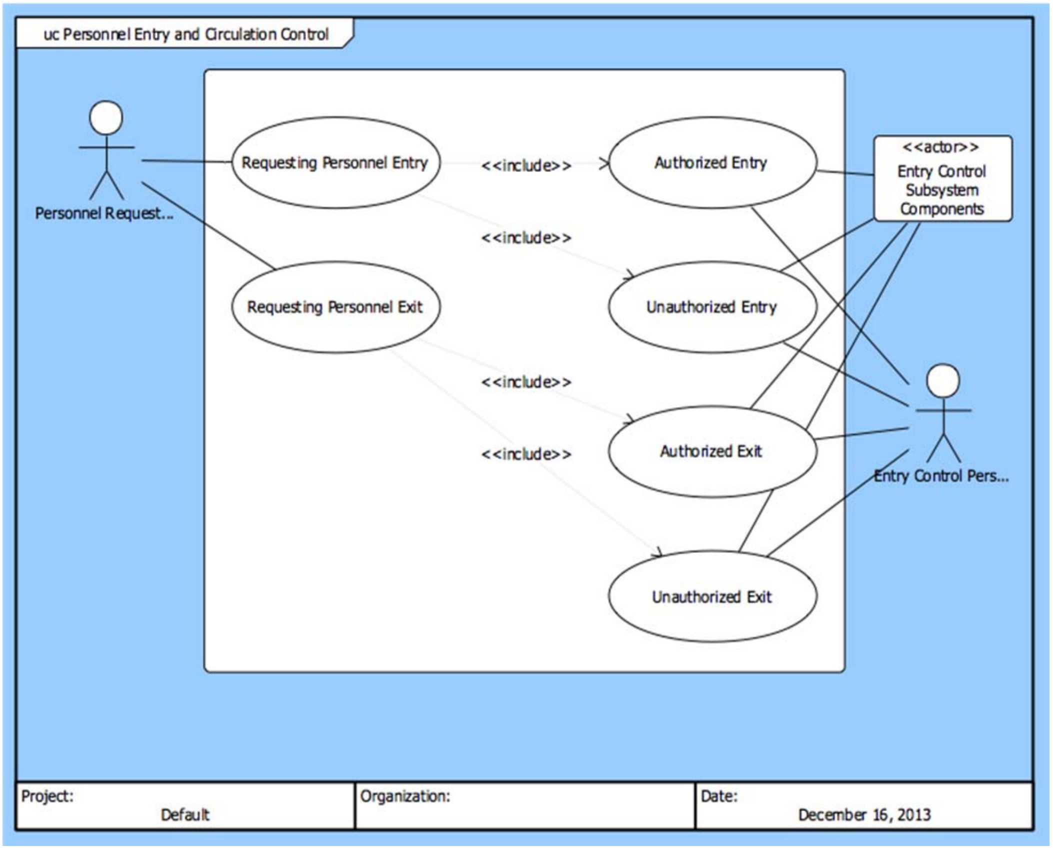


Figure 15. Use Case Diagram

The following use cases were utilized in the construct of the architecture:

Use Case: Requesting Personnel Entry

Primary Actor: Personnel Requesting Entry

Goal: To ascertain if the person is validly requesting entry, i.e., has valid credentials, has been authorized into the restricted area, is not under duress, and is not carrying contraband. Once confirmed, expeditiously process entry into the restricted area.

Preconditions: The primary actor has been enrolled into the system and the system can recognize the individual's smart card, authorization level, PIN, and biometric data. The person requesting entry needs to be carrying a valid smart card.

Trigger: The primary actor approaches the entry control point

Baseline Scenarios based on upon the included Authorized Entry:

1. Person Approaches entry control point.
2. Security force personnel recognize that the person is waiting processing and the isolated entrapment area is clear of other personnel.
3. Security force personnel unlock a gate that allow the person into the entrapment area with the gate securing behind him.
4. The person requesting entry inserts the smart card into a reader, enters a PIN into a PIN-Pad, and provides biometric data through a reader.
5. As required, the person places and hand-carried items through a contraband scanner and enters a body scanner.
6. Security Force personnel unlock gate on other side of entrapment area
7. Person enters the restricted area.

Included Scenario (Unauthorized Entry

1. If the person has invalid entry authorization, security force personnel notify him of this and the entry gate is unlocked so the invalid person retreats to the unsecure side of the control point.
2. If the person is deemed to have another individual’s Smart Card, he is detained as a security violator, and is passed to the security responses force.
3. If the person is determined to be under duress, the entry control point is secured from all activity and the security response force is deployed.
4. If the person is carrying contraband, he is detained, contraband is seized, and the security response force takes responsibility for the violator.

Scenario Variant (Authorized or Unauthorized Exit):

1. Vehicle approaches entry control point.
2. All passengers debark vehicle and process as personnel (the driver remains in the vehicle).
3. Security force personnel recognize that a vehicle is waiting processing and a vehicle entrapment lane is empty.
4. Security force personnel open the gate to the vehicle entrapment area.
5. The driver drives the vehicle into the entrapment area.
6. The driver stops the vehicle, shuts off the vehicle, and removes the ignition key.
7. Security force personnel shut the vehicle entrapment area gate.
8. The driver proceeds to open all compartments within the vehicle, including but not limited to, glove box, hood, job boxes, and packages.
9. The driver moves to the personnel queue and processes as a dismounted person.
10. A security force sentry utilizes contraband scanners to search all compartments for contraband.
11. Once a compartment is searched the security force member shuts the compartment.
12. Once the driver successfully processes as a dismounted person, he moves to a holding zone until the vehicle is completely searched.
13. The vehicle sentry signals the driver forward.
14. The driver gets into the vehicle.
15. The security force personnel open the opposite vehicle entrapment area gate.
16. The driver drives the vehicle out of the entrapment area into the restricted area and waits for any passengers to complete screening and re-enter the vehicle.
17. The security force secures the vehicle entrapment area exit gate.

3. Operational Activity Models

The operational activity models include the performers, organization, data flow between the performers, and a process compliant with requirements.

4. Performer Context Diagram and Organizational Relationships

ARAECS considers the interactions of five groups of performers. Of these five groups, two are inherent to the system and three are external stakeholders.

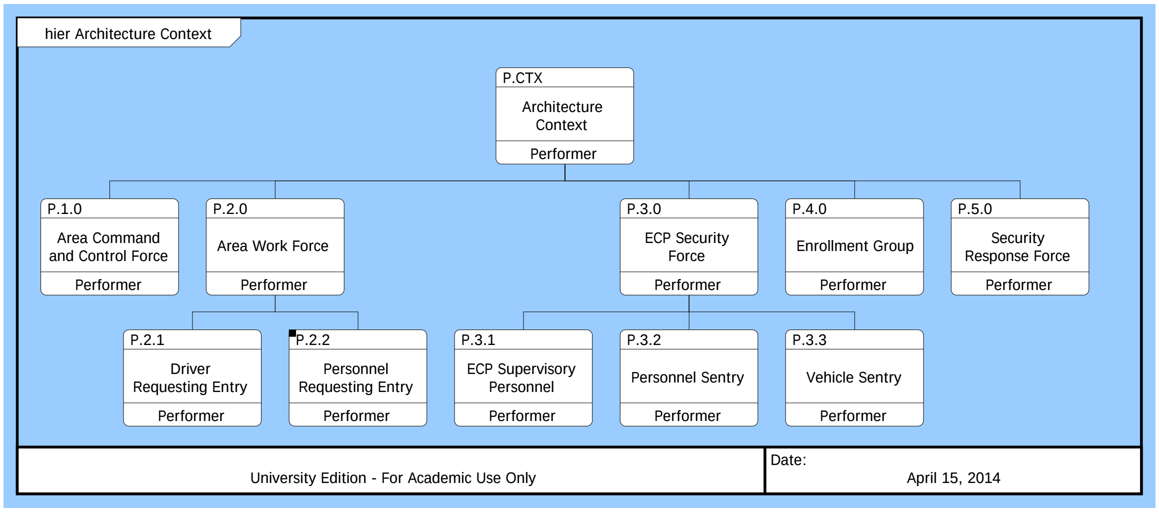


Figure 16. Organization of Operational Performers

Primary Performers:

- P2.0 Area Work Force. These are the individuals that require procedural access to the restricted area in the conduct of their duties. They may be drivers or dismounted.
- P3.0 ECP Security Force. These are the security force members that run the entry and circulation control. They monitor activities at their assigned entry control points, screen individuals, and operate the gates and screening equipment.

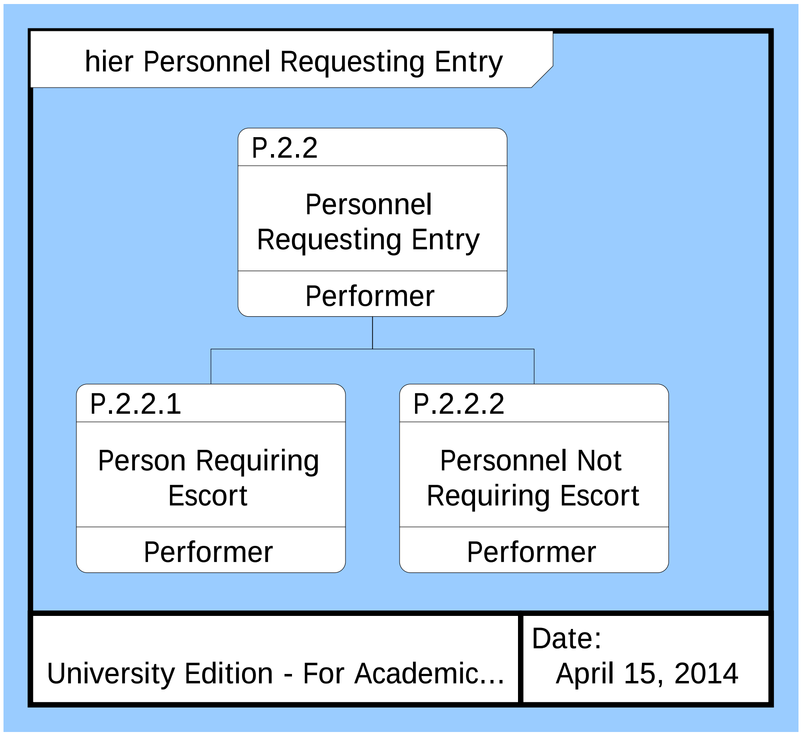

hier Personnel Requesting Entry
P.2.2
Personnel Requesting Entry
Performer
P.2.2.1
Person Requiring Escort
Performer
P.2.2.2
Personnel Not Requiring Escort
Performer
University Edition - For Academic...
Date:
April 15, 2014

Figure 17. Hierarchy of Varying Types of Performers Requesting Entry

External Stakeholders:

- P1.0 Area Command and Control Force. This is the segment of the security force that is monitoring communications and activities across the entire restricted area. This includes net control for wireless radio communications, alarms on structures and perimeter fencing, and reports from random patrols. The ECP Security Force communicates with the Area Command and Control Force.
- P4.0 Enrollment Group. These personnel collect primary identification, validate that information, and enter it into the authorized database prior to the Area Work Force gaining access to the restricted area.
- P5.0 Security Response Force. This is a ready-alert segment of the guard force that is ready to respond to any security threat and defeat it. The Security Response Force responds to security violations at the entry control point.

5. ARAECS External Activity Interfaces and Level 1 Data Flow

The top level interface and operational data flow diagram highlights the connectivity between the operational architecture and the external performers. Note that the Area Work Force is in the use case, but for the purposes of the design methodology, they are external performers.

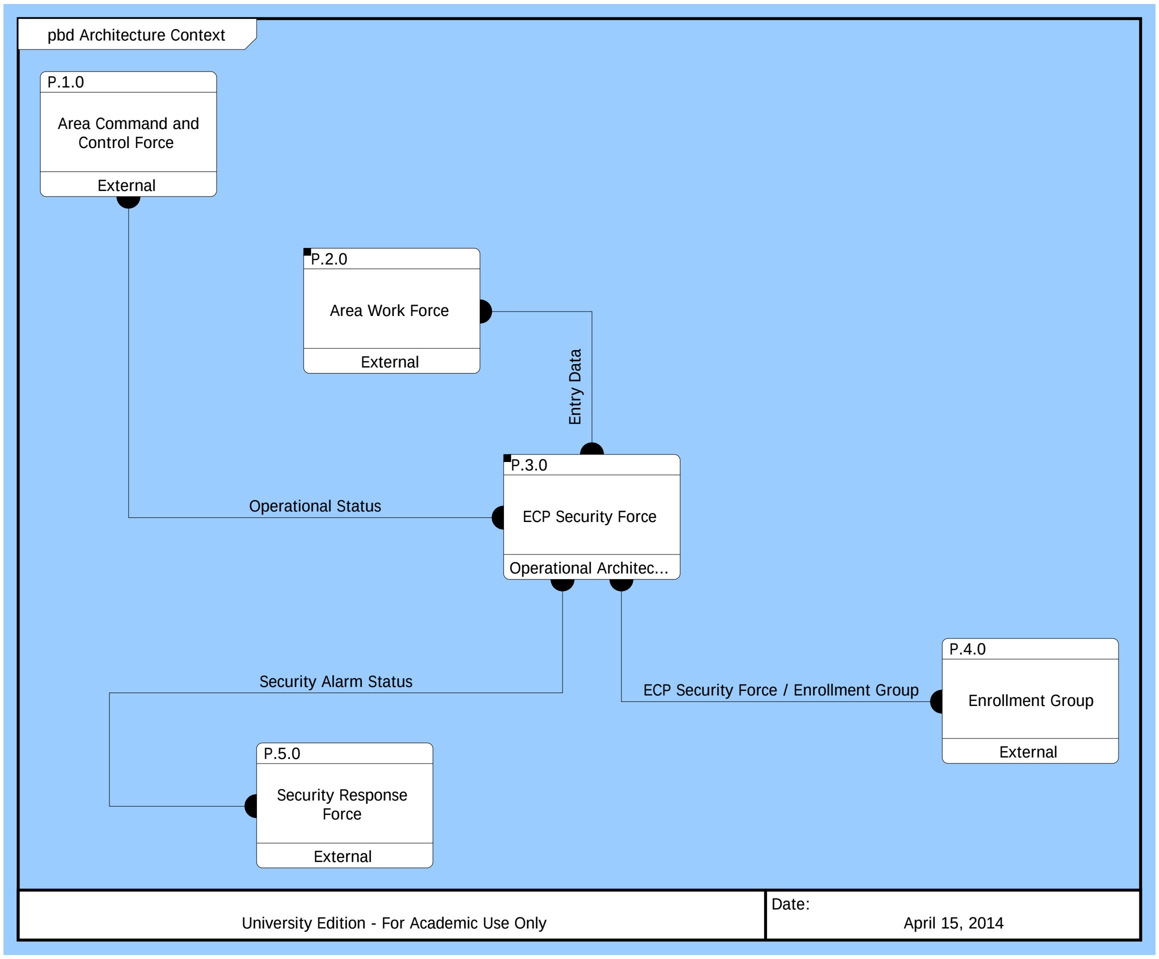


Figure 18. Level I Data Flow Between Operational Performers

a. Operational Activity Sequencing

The following operational processes were derived from the requirements documentation. Per the use cases, exiting processes largely mirror entry processes.

The basic requirements for entry include interfacing with a physical perimeter boundary and sending all personnel to an identified entry control point. At that point, personnel are segregated and must be checked for a valid badge, valid authorization to enter the restricted area, and must be free of contraband or duress.

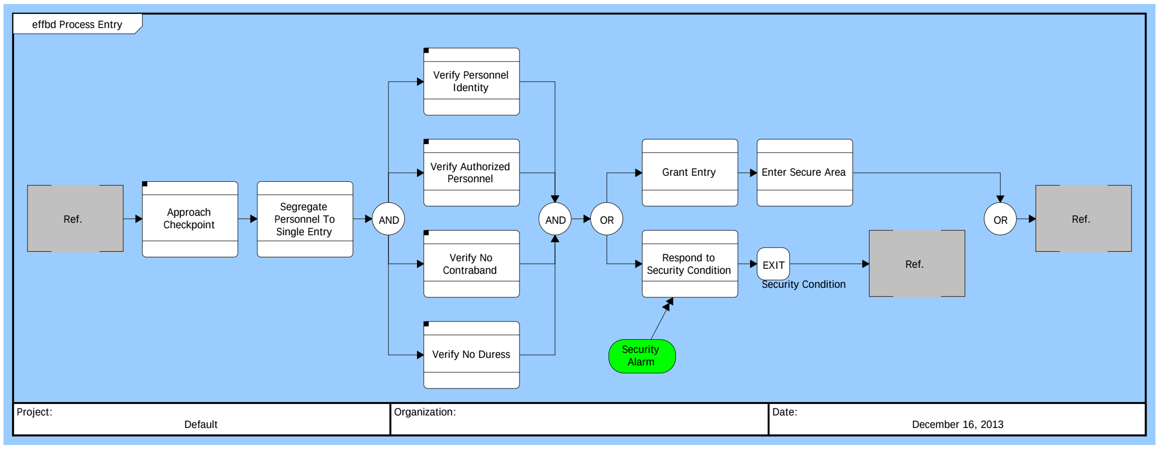


Figure 19. Required Operational Behavior Processes

The four principal operational activities of the entry/exit process are further decomposed.

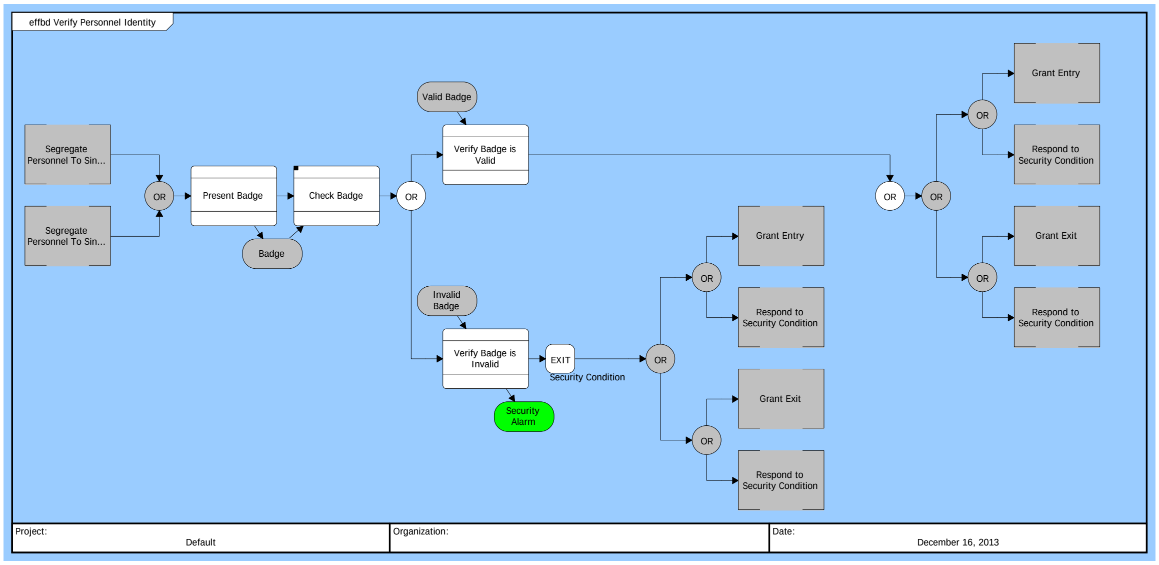


Figure 20. Personnel Identity Validation Behavior

An invalid badge is cause for a security response. Invalid in this context can indicate that the person does not have a badge, the badge is expired, the person is using another person's badge, or the badge is counterfeit. The following decomposition looks for these situations.

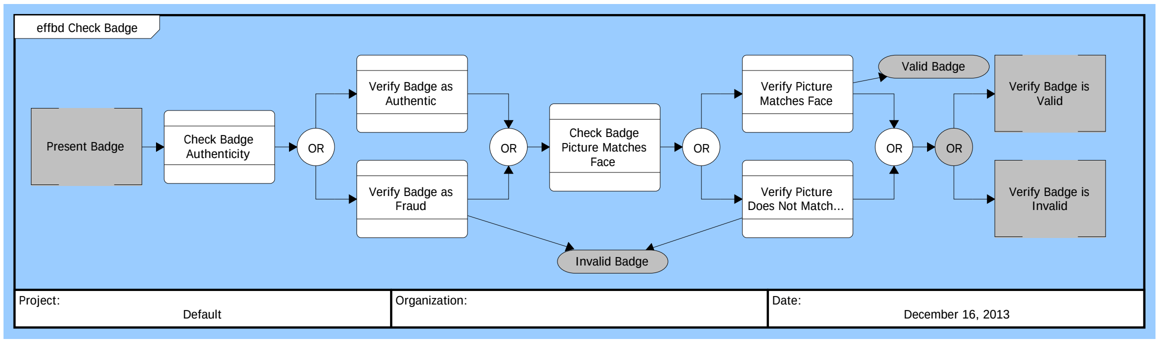


Figure 21. Badge Validation Behavior

A valid badge does not necessarily indicate that authorization is granted. Multi-use badges (such as the Common Access Card (CAC)) have varying levels of authorization (i.e., even though all personnel have a CAC, different individuals may have different levels of access as encoded onto the CAC). Therefore, the system, in addition to validating the badge, must separately validate access authorization. A restricted area typically has two main levels of access: full entry (no escort required) or limited entry (escorted access only).

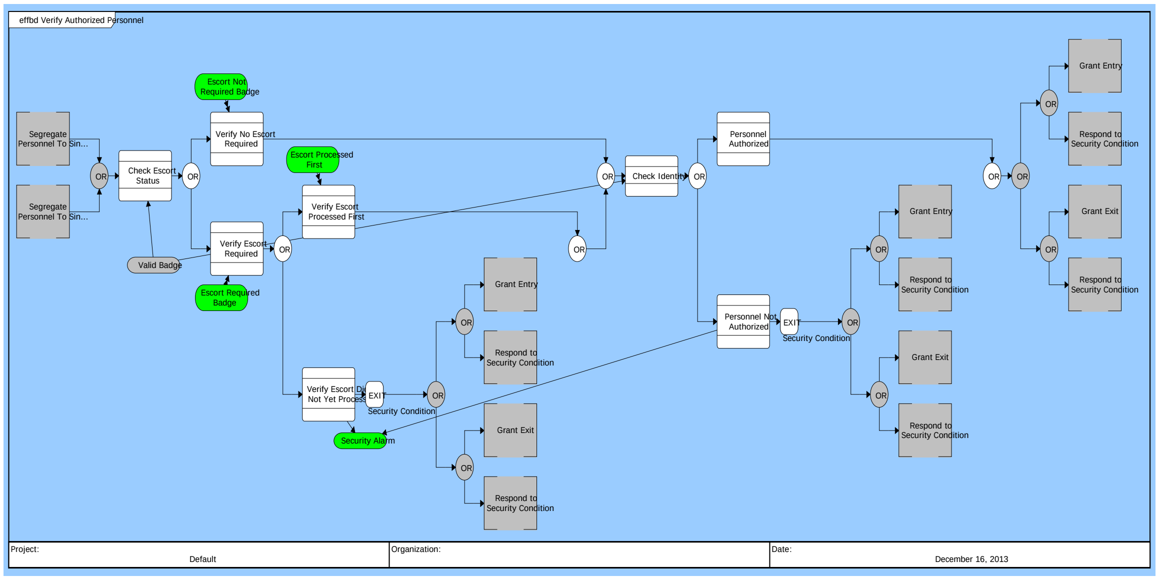

effbd Verify Authorized Personnel
Segregate Personnel To Sin...
Segregate Personnel To Sin...
OR
Check Escort Status
Valid Badge
OR
Escort Not Required Badge
Verify No Escort Required
Escort Processed First
Verify Escort Processed First
Verify Escort Required
Escort Required Badge
OR
Verify Escort Did Not Yet Process
EXIT
Security Condition
Security Alarm
OR
OR
Grant Entry
Respond to Security Condition
OR
Grant Exit
Respond to Security Condition
OR
OR
Check Identity
OR
Personnel Authorized
Personnel Not Authorized
EXIT
Security Condition
OR
OR
Grant Entry
Respond to Security Condition
OR
Grant Exit
Respond to Security Condition
OR
OR
OR
Grant Entry
Respond to Security Condition
OR
Grant Exit
Respond to Security Condition
Project:
Default
Organization:
Date:
December 16, 2013

Figure 22. Contraband Screening Behavior

This process highlights the selection for detailed or cursory searches for contraband.

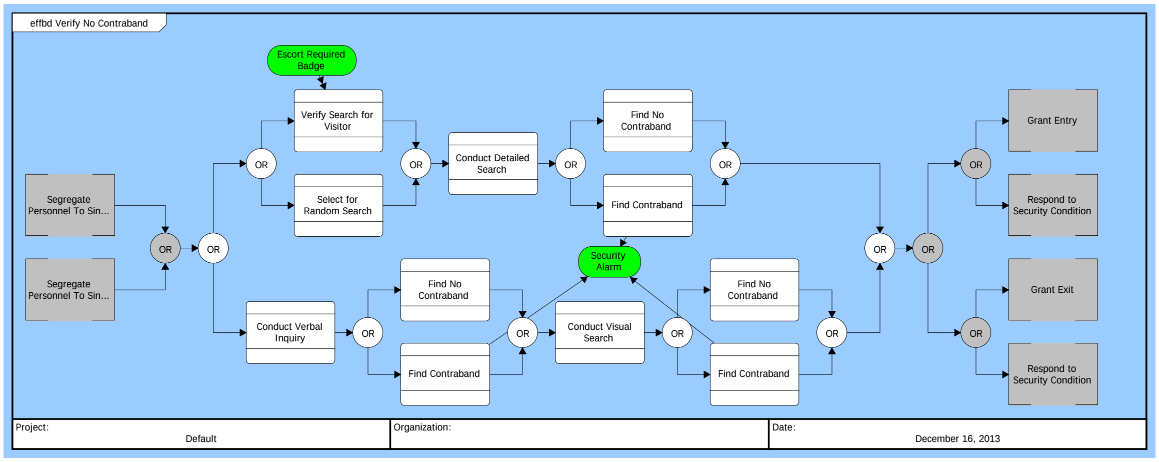


Figure 23. Behavior Variances for Personnel Requiring Escort

The final operational process decomposition addresses duress, or, the threat of violence to compel someone to knowingly violate security procedures. There are typically several methods to indicate duress in a security environment to include answering obvious questions ("Are you under duress?") to passing a covert word or phrase in a seemingly routine statement (such as a comment about the weather). There are also physical duress alarms. As the ARAECS segregates personnel into an entrapment area, the use of more obvious indications of duress can be effective. However, sometimes the person under duress has received threats to family members or others who are not physically present—so even though the person is segregated, he may still be under duress conditions.

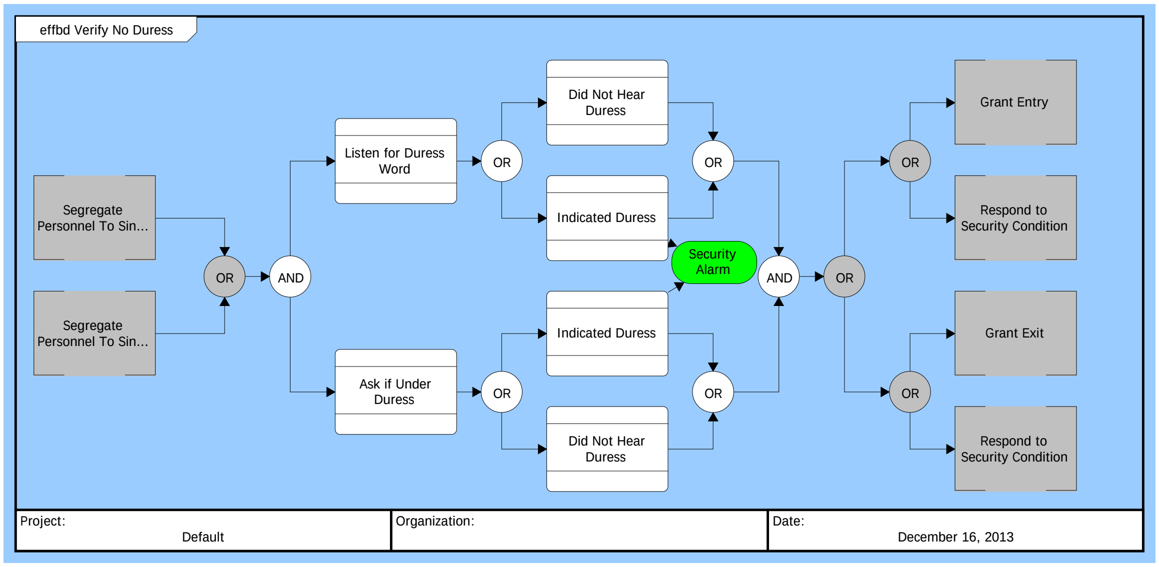


Figure 24. Duress Challenge Behavior

6. System Functionality Description

The objective of the system-functional portion of the architecture is to indicate how the ARAECS reflects the operational requirements and processes that have been identified. It takes into account the combined manpower-technology-physical nature of the ARAECS to accomplish the overall mission objectives.

a. Functional Context and Hierarchy

(1) Functional Context—Level 0. The functional context exists within the overall Prime Directive of establishing and maintaining a secure restricted area. The area must be defined with a controlled boundary. Security forces must be aware of potential threats within the area, respond to them, and defeat them. These aspects are provided through situational awareness, communicated through all response nodes, and an established capability within the responding forces to defeat threats.

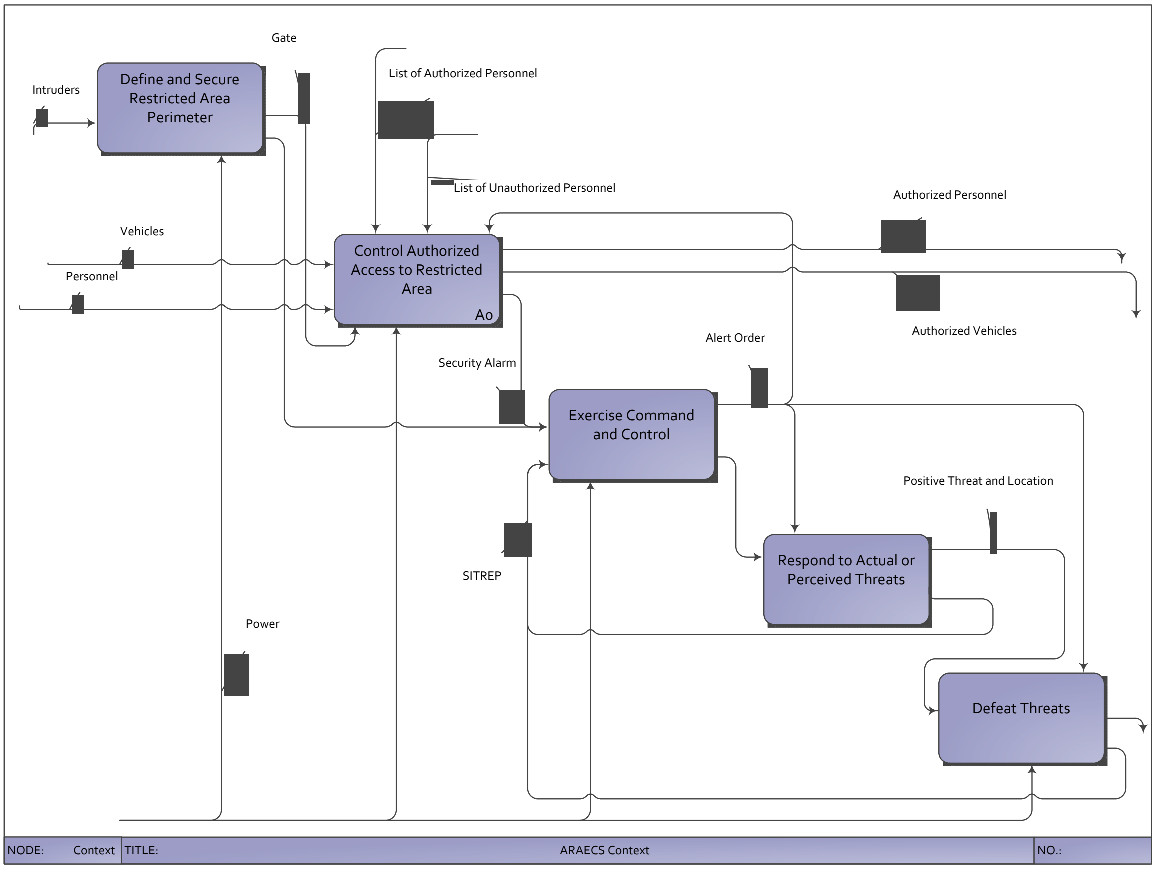

Gate
Intruders
Define and Secure Restricted Area Perimeter
List of Authorized Personnel
List of Unauthorized Personnel
Authorized Personnel
Vehicles
Personnel
Control Authorized Access to Restricted Area
Ao
Authorized Vehicles
Alert Order
Security Alarm
Exercise Command and Control
Positive Threat and Location
SITREP
Respond to Actual or Perceived Threats
Power
Defeat Threats
NODE: Context
TITLE: ARAECS Context
NO.:

Figure 25. ARAECS in Context With the Overall Security System

(2) Functional Hierarchy—Level 1 Decomposition. Since restricted areas need to exist concurrent with ongoing operations, such as ship refit, the boundary must allow controlled passage between the secure and unsecure sides. This is A_0, or the zone with which ARAECS operates. While ARAECS will require some of the same capabilities of the overall system (or system of systems), it will require its own organic design within the access control protocol.

Level 1 decomposition of the overall context provides the basic level of functional requirements for ARAECS.

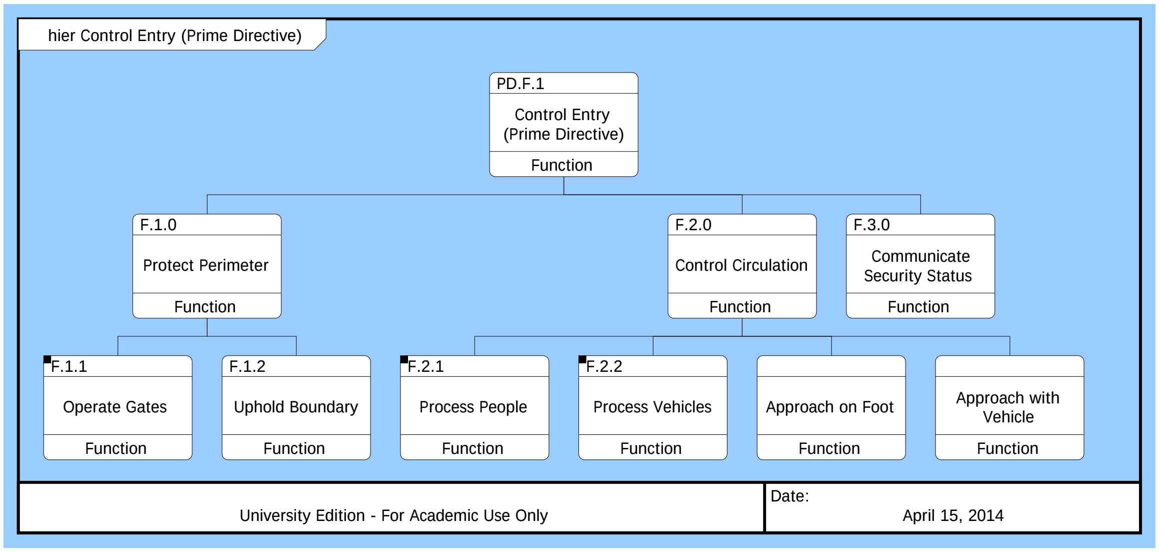


Figure 26. Functional Hierarchy to Support the ARAECS Prime Directive

Since controlled entry across a boundary exists at the boundary itself, ARAECS must integrate with the adjacent boundary subsystems and provide its own perimeter protection and situational awareness.

Circulation control is the functional heart of the system, because its decomposed functions must meet the directed requirements for access, identify authorized access requests, and allow rapid boundary passage for authorized entrants.

The ARAECS system must communicate with the overarching system or SoS. Per the operational architecture, the system must receive communications to determine if personnel requesting access are authorized. If security violations are found, ARAECS must communicate the situation to the overarching system and integrate with the security response function to defeat the threat before unauthorized access is achieved.

(3) Functional Hierarchy– Level 2 Decompositions.

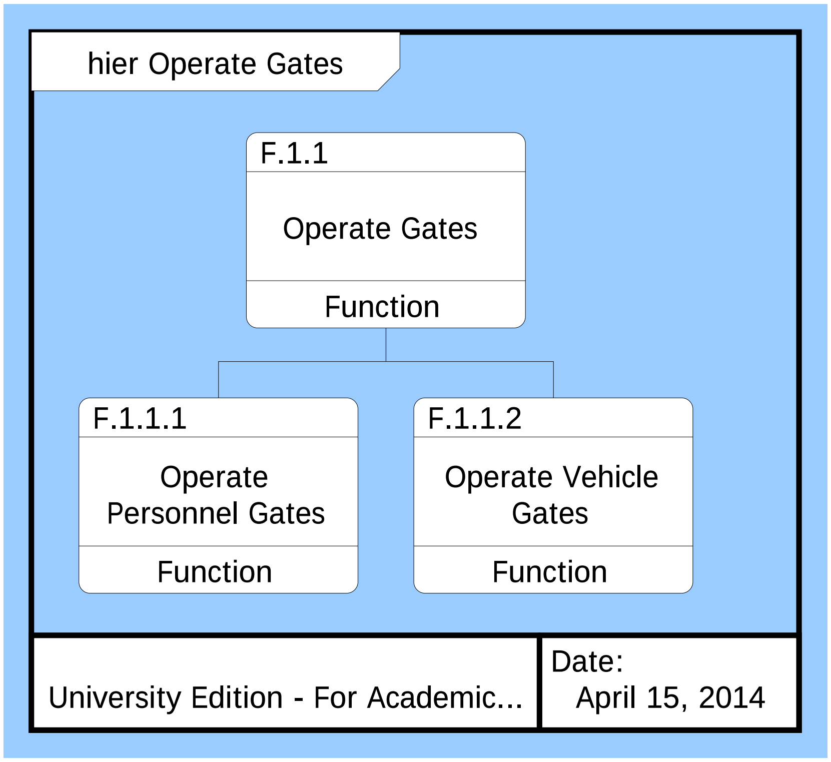


Figure 27. Functional Decomposition for Gate Operation

To achieve the requirements of ARAECS, the gate function must accommodate both vehicles and dismounted personnel.

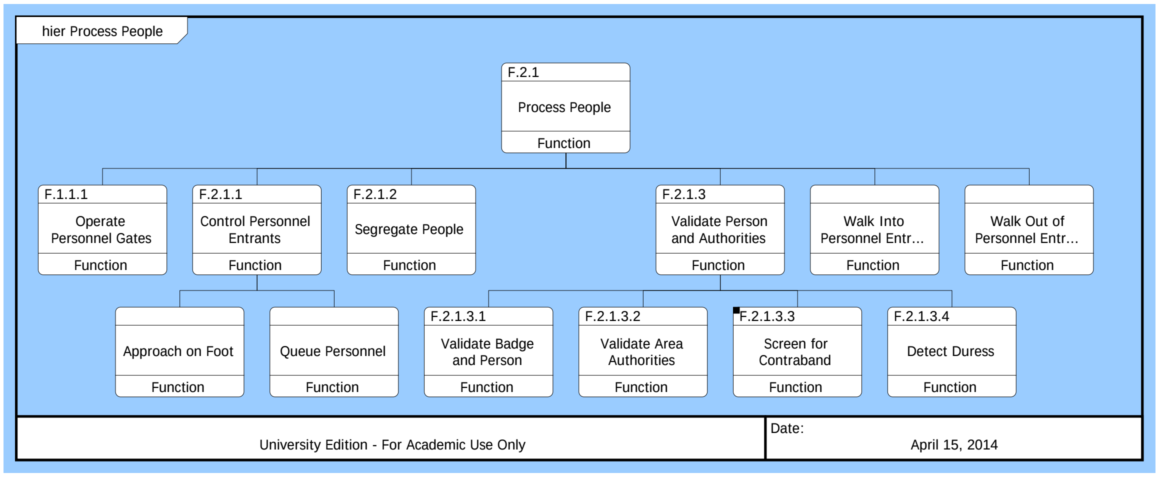


Figure 28. Functional Decomposition for Processing People

The Process People function is one of the most complex system functions. The operational activity diagram leverages the Process People function by nesting personnel access functions within the overall context of processing vehicles, i.e., drivers exit their vehicle and enter the Process People function prior to returning to their screened vehicle.

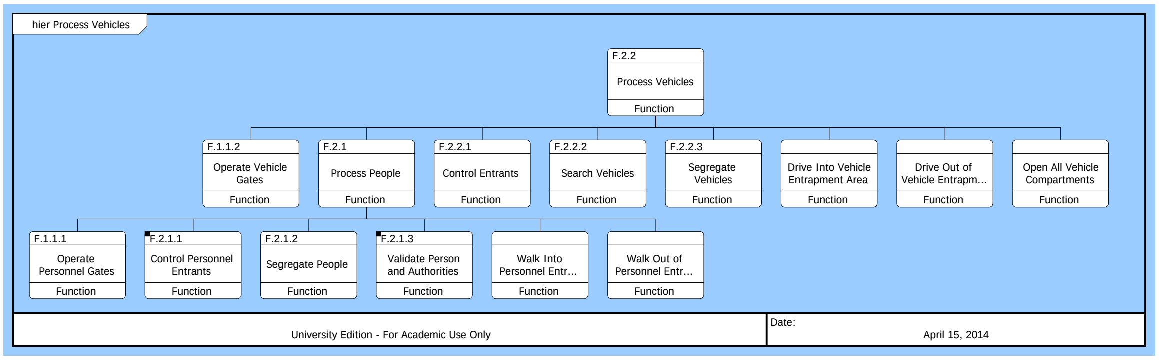


Figure 29. Functional Decomposition for Processing Vehicles

(4) Functional Hierarchy—Level 3 Decomposition. The four primary security protocols are nested within the third level system function of Validating Person and Authorities. Further decomposition of the Screen for Contraband function delineates the requirement to provide both cursory and detailed searches for contraband. Hybrid-B takes advantage of the time savings that a cursory search provides by allowing personnel with an adjudicated clearance to take advantage of this expedited search and focusing the most resource intensive searches on those without background checks.

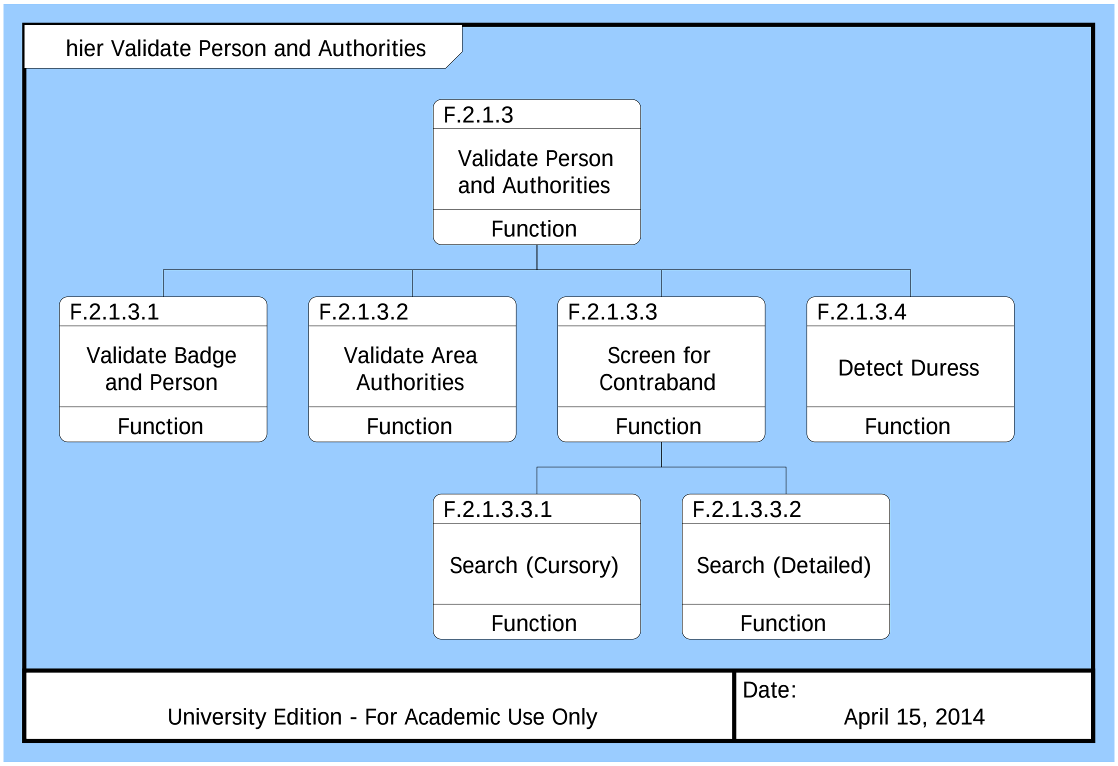


Figure 30. Functional Decomposition for Validating Personnel

7. System Functional Performance Description

Enhanced Functional Flow Block Diagrams (EFFBD) are used to augment the operational architecture by showing analogous use of system functions, mapped to system components to achieve the Prime Directive

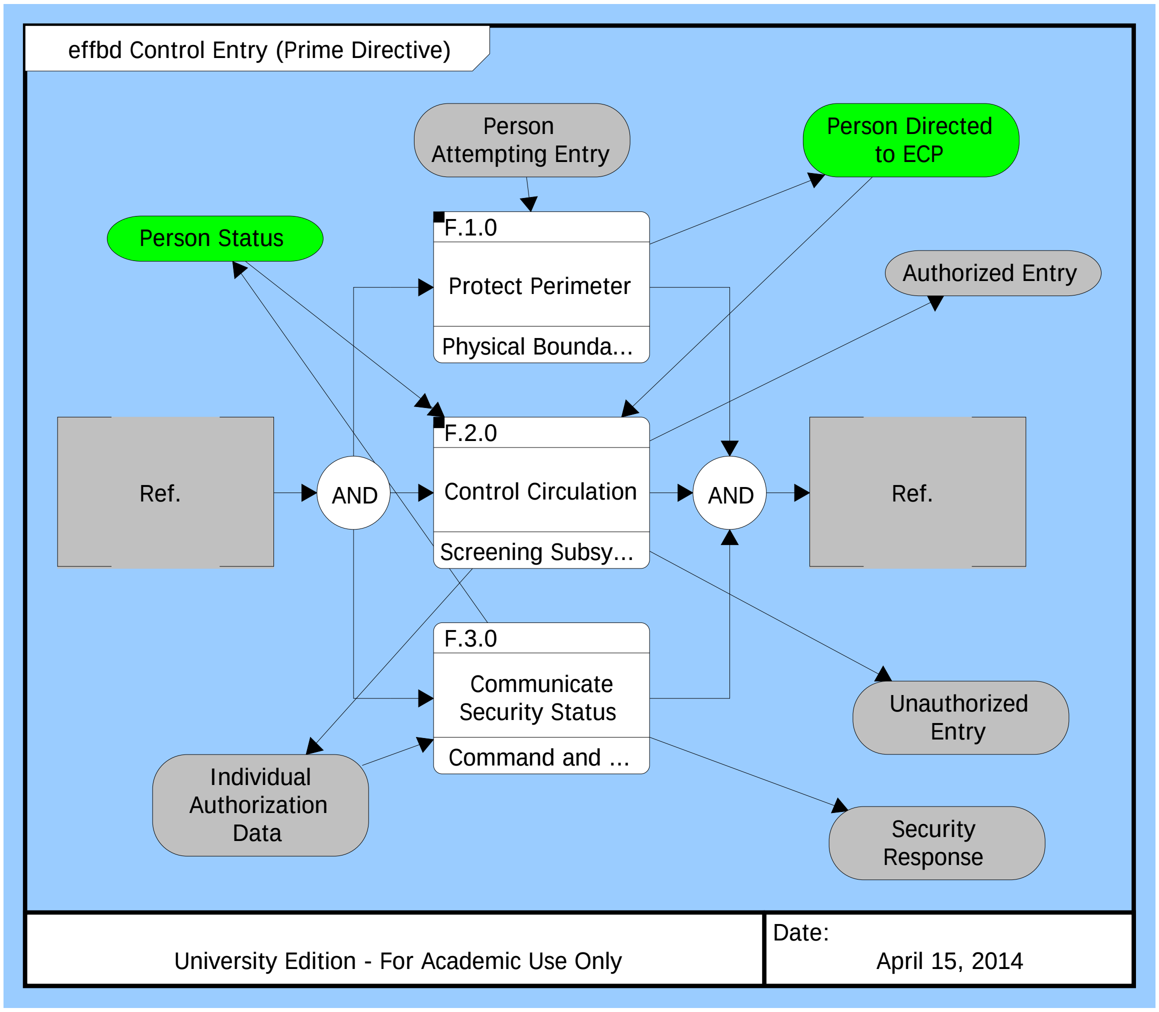


Figure 31. Behavioral Diagram of the ARAECS Prime Directive

The overall relationship of the top-level system functions decomposed from the Prime Directive are parallel in nature. ARAECS must concurrently maintain the system boundary, even while controlling circulation and keeping the overarching security system aware of the situation.

The system architecture in the next two diagrams examines the system functions allocated to the external system stakeholders with regard to personnel attempting authorized access with and without vehicles.

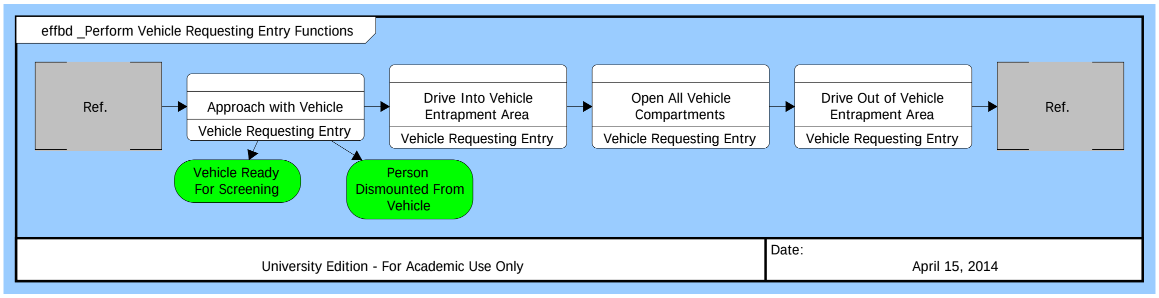

effbd _Perform Vehicle Requesting Entry Functions
Ref.
Approach with Vehicle
Vehicle Requesting Entry
Drive Into Vehicle Entrapment Area
Vehicle Requesting Entry
Open All Vehicle Compartments
Vehicle Requesting Entry
Drive Out of Vehicle Entrapment Area
Vehicle Requesting Entry
Ref.
Vehicle Ready For Screening
Person Dismounted From Vehicle
University Edition - For Academic Use Only
Date:
April 15, 2014

Figure 32. Functional Behavior From the Perspective of a Vehicle Requesting Entry

A vehicle requesting entry must approach, disembark passengers, drive into and out of the entrapment area, and prepare vehicle compartments for inspection.

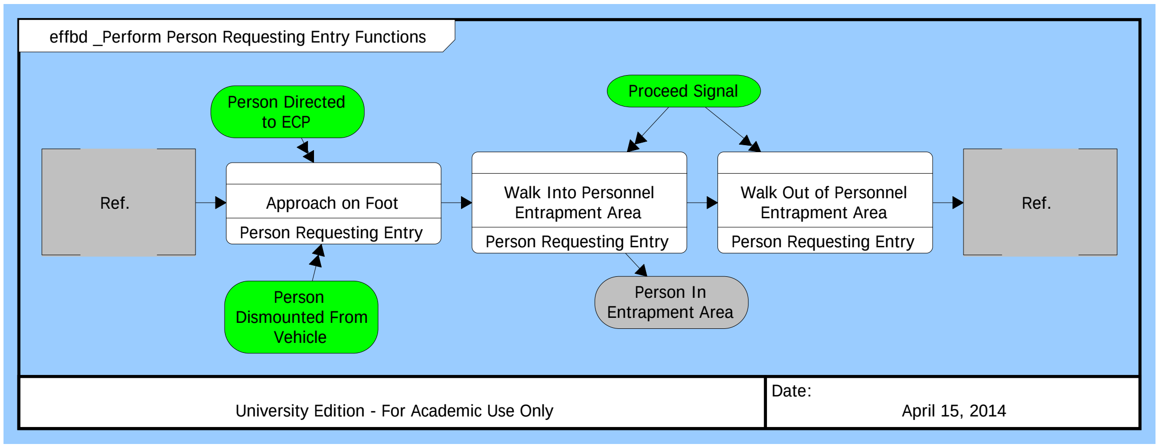

effbd _Perform Person Requesting Entry Functions
Person Directed to ECP
Proceed Signal
Ref.
Approach on Foot
Person Requesting Entry
Walk Into Personnel Entrapment Area
Person Requesting Entry
Walk Out of Personnel Entrapment Area
Person Requesting Entry
Ref.
Person Dismounted From Vehicle
Person In Entrapment Area
University Edition - For Academic Use Only
Date:
April 15, 2014

Figure 33. Functional Behavior From the Perspective of a Personnel Requesting Entry

Personnel on foot must approach, and upon alert by signals from ARAECS, proceed into and out of the entrapment area.

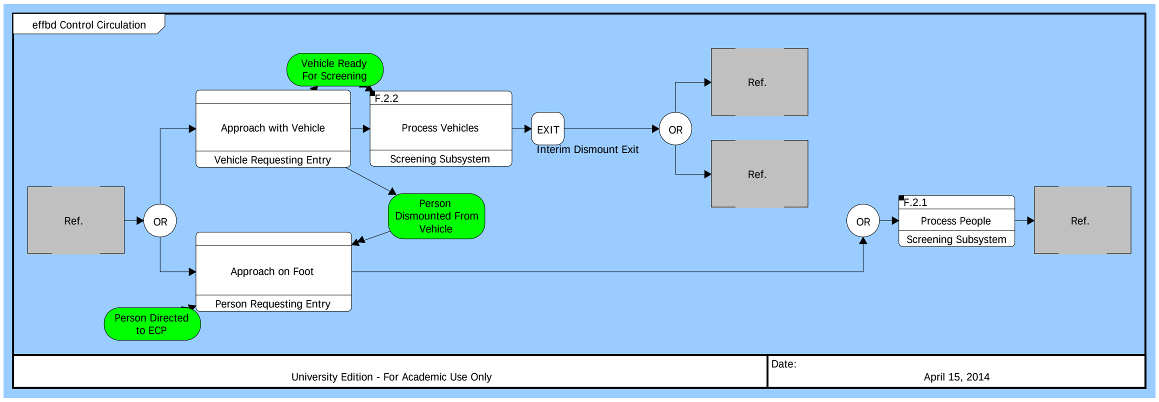


Figure 34. Functional Behavior for Initiating the Screening Process

From the perspective of ARAECS functions allocated to the screening system, system functions must work in concert with the external stakeholders' actions. During detailed design, particular attention must be paid to these interfaces between the ARAECS and personnel requesting entry so that signals are clear and unambiguous.

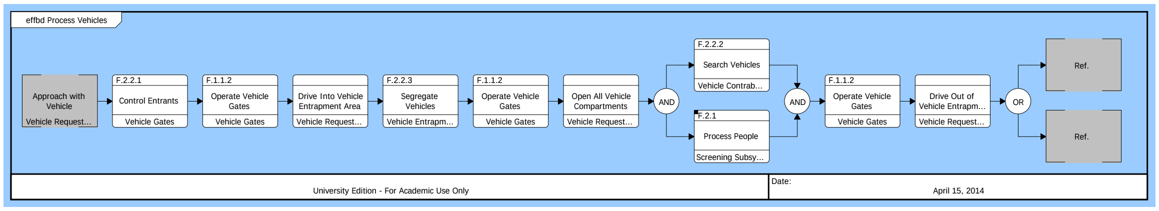


Figure 35. Functional Behavior for Processing Vehicles

The Process Vehicles function includes a complex series of tasks that take place in concert with the personnel validation process for the driver. Since the modeled behavior requires the driver to accomplish steps that lead to the vehicle being prepared for inspection within an entrapment area, the driver's entry validation occurs as the vehicle is searched.

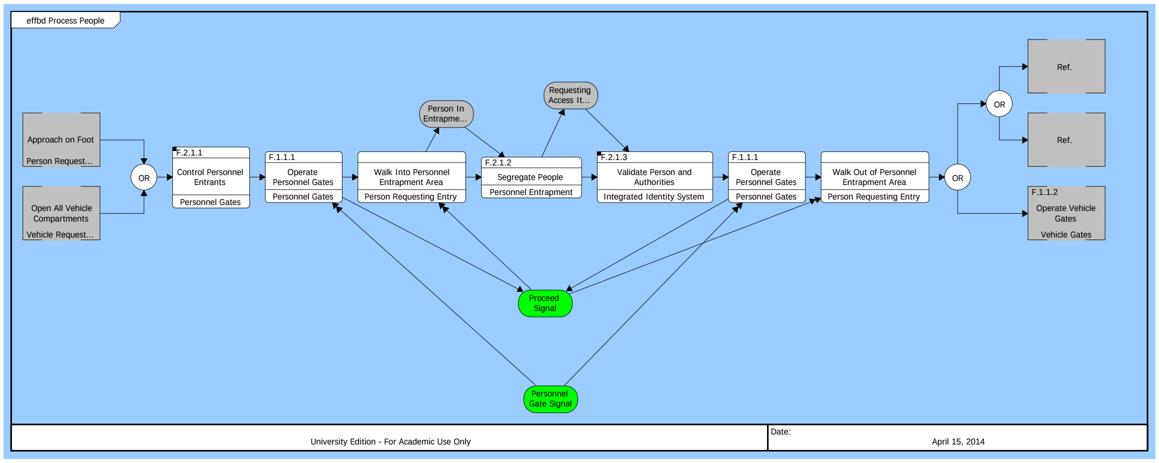


Figure 36. Functional Behavior for Processing People

When functional behavior is integrated between the external stakeholder and ARAECS, a more complete view of the interrelationships between the person requesting access and the system components can be identified.

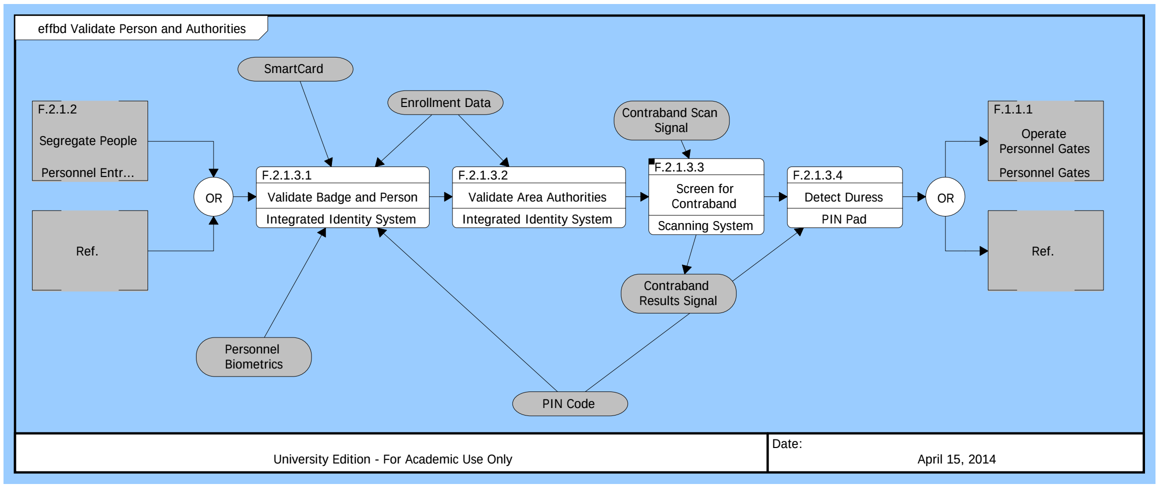


Figure 37. Functional Behavior Decomposition for Validating Personnel

The critical procedure of establishing authorized access is decomposed within the Process People function through the validation of the person and their authorities. This system behavior decomposes to the four principal security protocols of validating badge, validating authorities, screening for contraband, and detecting duress.

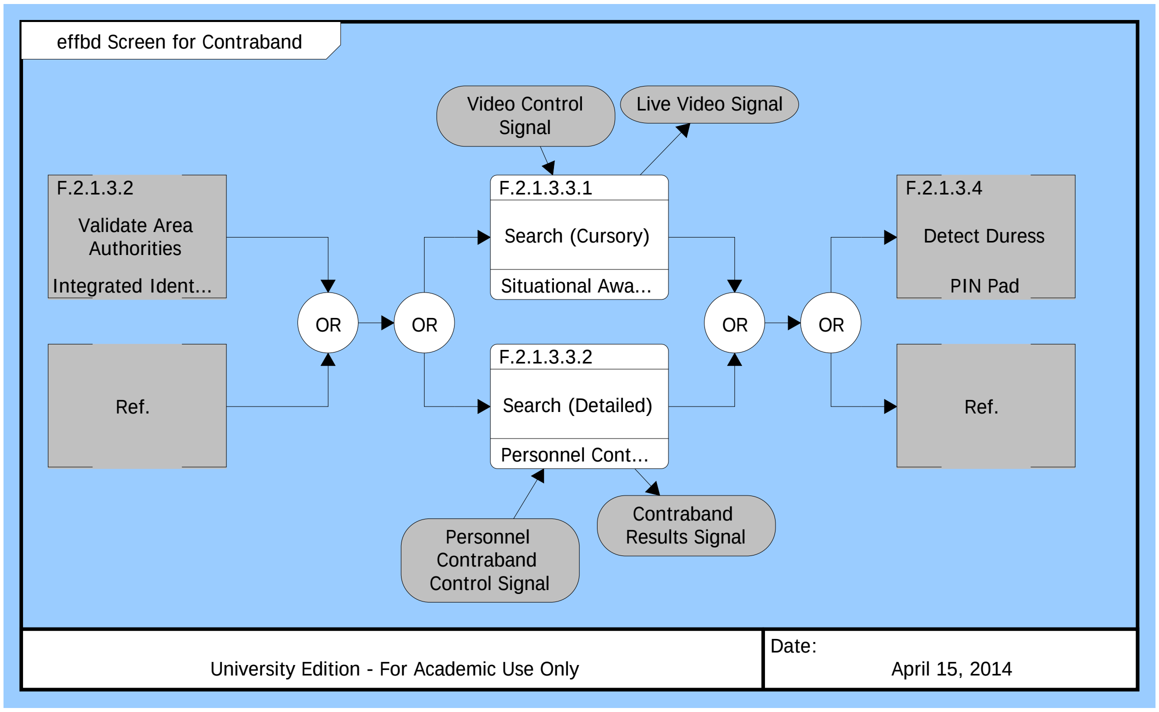


Figure 38. Functional Behavior Decomposition for Contraband Screening

As Hybrid-B relies upon a dual method of screening for contraband, this figure indicates the need for differing inputs and outputs, which at the component level will ultimately require the need for differing system component interfaces and linkages.

8. System Component Descriptions

The functional EFFBDs identified the behavior of system functions that comply with the operational architecture. These functions are allocated to discrete system component hierarchies. Detailed design will refine these hierarchies and make system acquisition choices on hardware that will fulfill their functions, as allocated within the architecture. Specific hardware choices potentially mandate design changes. The team’s technology research will help to inform decisions on specific hardware.

a. System Component Hierarchies

For simplicity, component hierarchy mirrors the three function decomposition approach of the ARAECS.

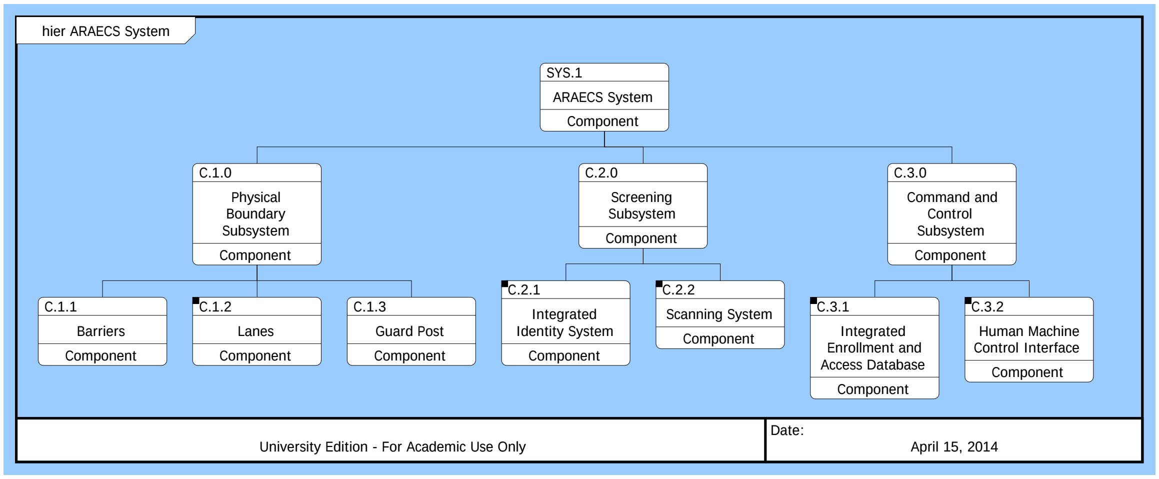


Figure 39. ARAECS Top-Level Component Hierarchy

Since ARAECS must accomplish three major functions, these were allocated to three major subsystems.

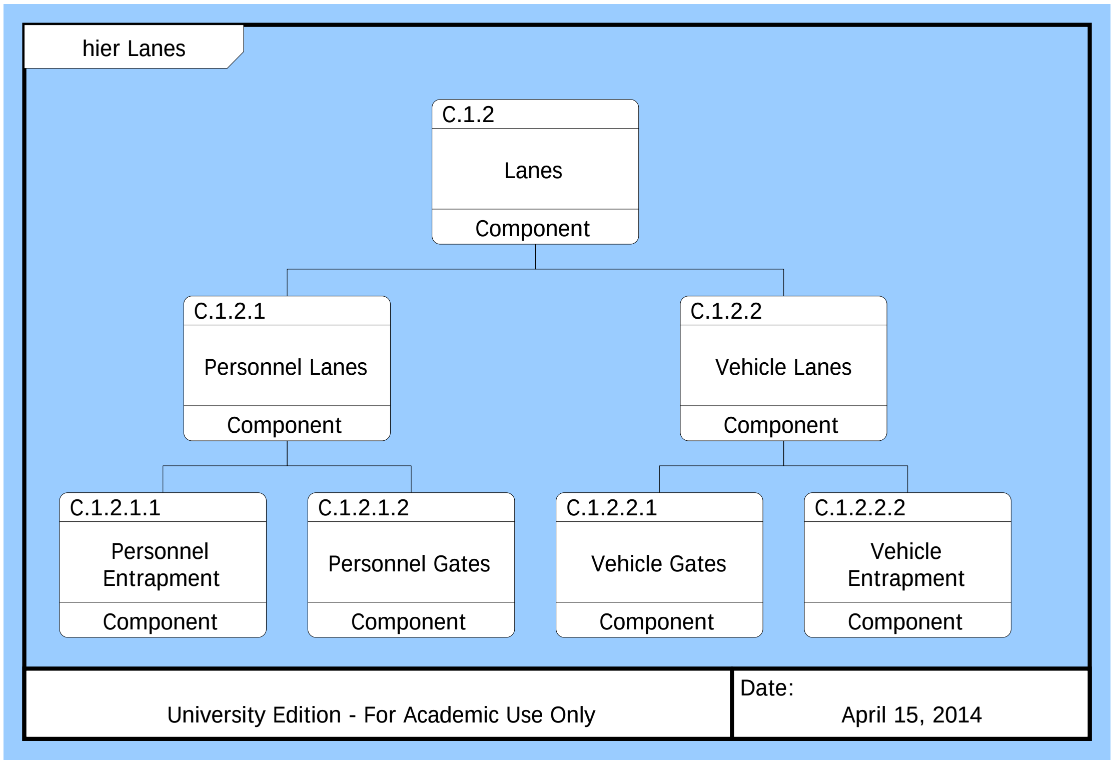


Figure 40. Lane Component Hierarchy

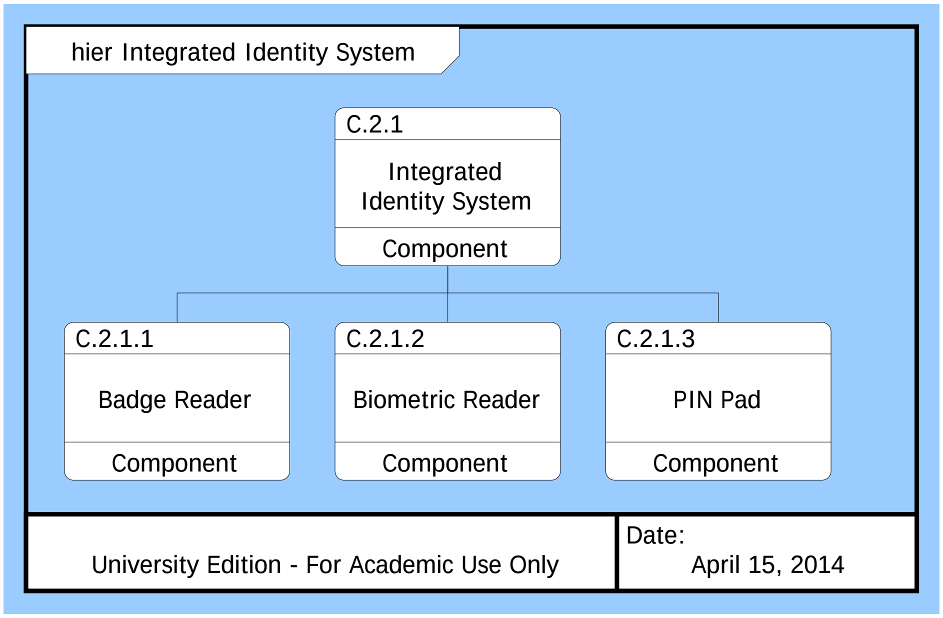


Figure 41. Integrated Identity System Hierarchy

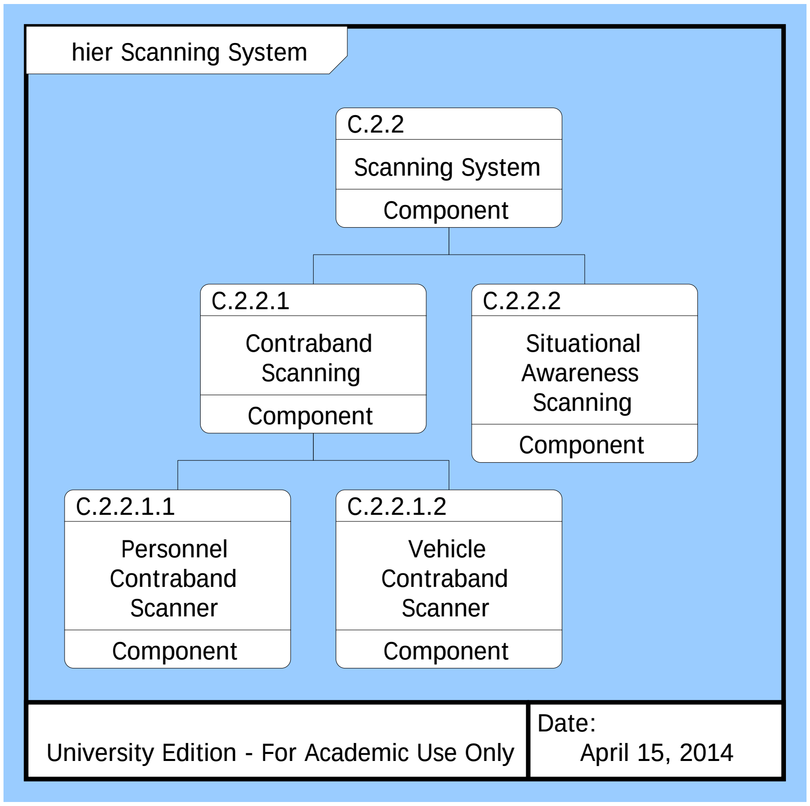


Figure 42. Scanning Component Hierarchy

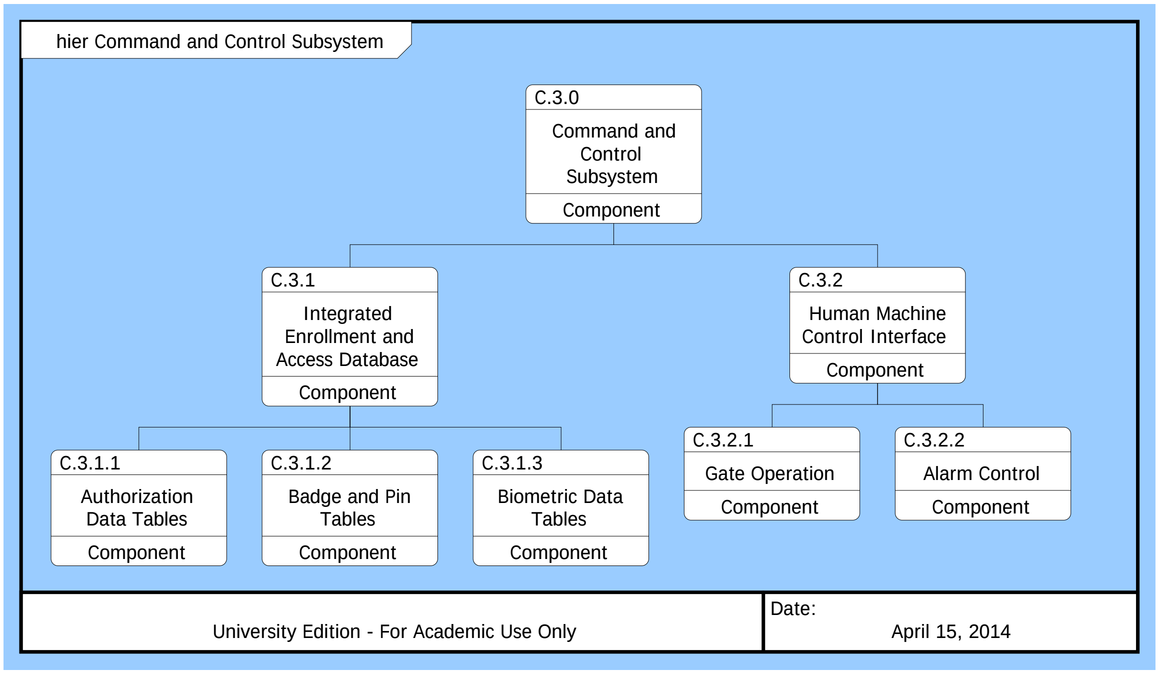


Figure 43. Command and Control Subsystem Hierarchy

b. Systems Connections Interfaces

ARAECS conceptual design looked at the basic system interfaces between the top level system components. The functional EFFBDs, based upon the operational architecture, identified the need for multiple, reliable, and unambiguous interfaces between the ARAECS and external stakeholders requesting entry and exit. Detailed design will require further work, and the system selection (COTS, purpose built, Operating System) will drive many of these design choices.

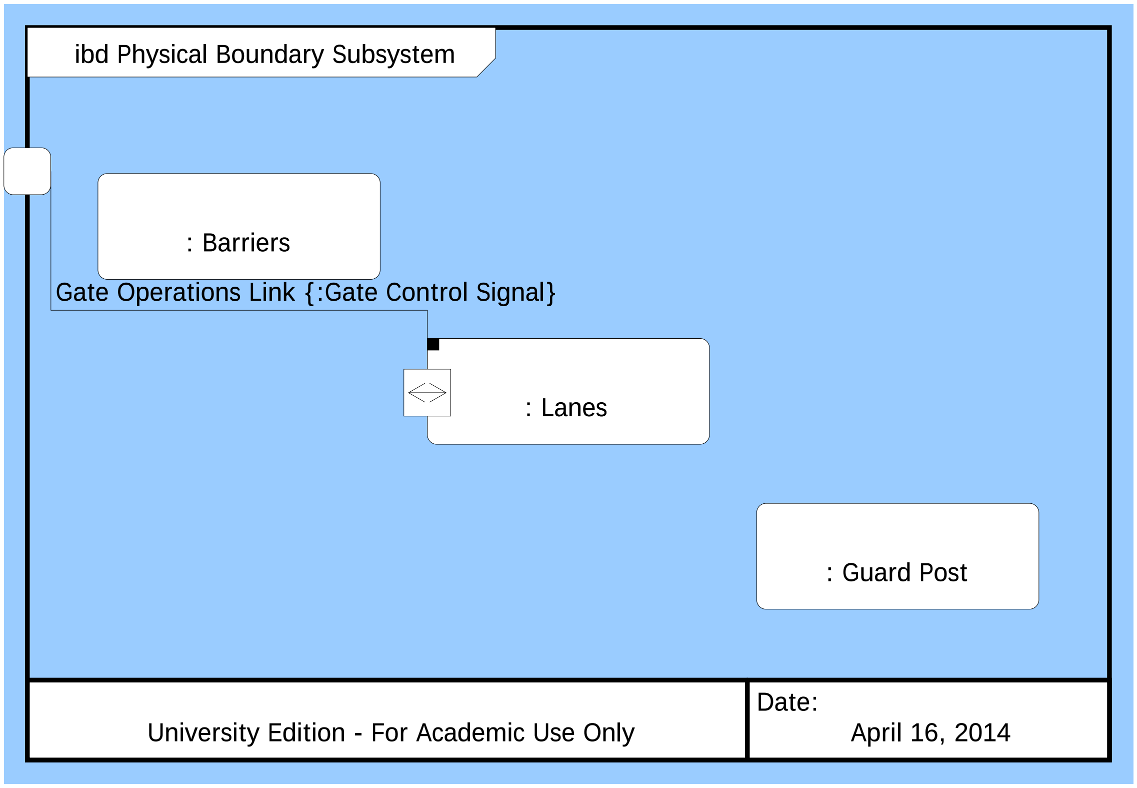

ibd Physical Boundary Subsystem
: Barriers
Gate Operations Link {:Gate Control Signal}
: Lanes
: Guard Post
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 44. Physical Boundary Subsystem Interfaces

Interfaces with the physical boundary subsystem identify the passive nature of the barriers and the guard post in upholding the boundary. Entry and exit lanes, as well as movable gates within the personnel and vehicle lanes, require interface to a control system.

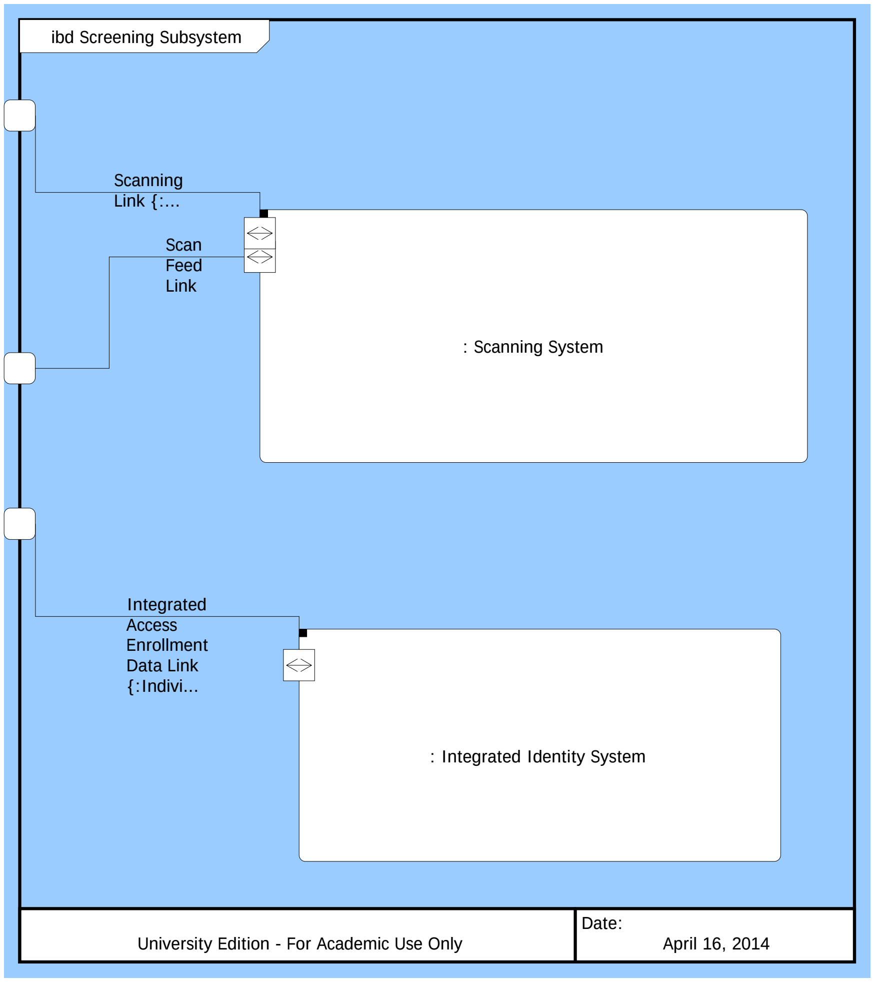

ibd Screening Subsystem
Scanning Link {:...
Scan Feed Link
: Scanning System
Integrated Access Enrollment Data Link {:Indivi...
: Integrated Identity System
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 45. Screening Subsystem Interfaces

The screening system relies upon two major linkages. The identity system must transfer the information (identity, access level, biometrics, PIN) to the enrollment system to validate authorized access. The scanning system must transfer the results of the contraband search to the operator to validate that no contraband is being introduced. Since the contraband system relies upon two types of scans, the detailed design must identify the best methods to transfer this information.

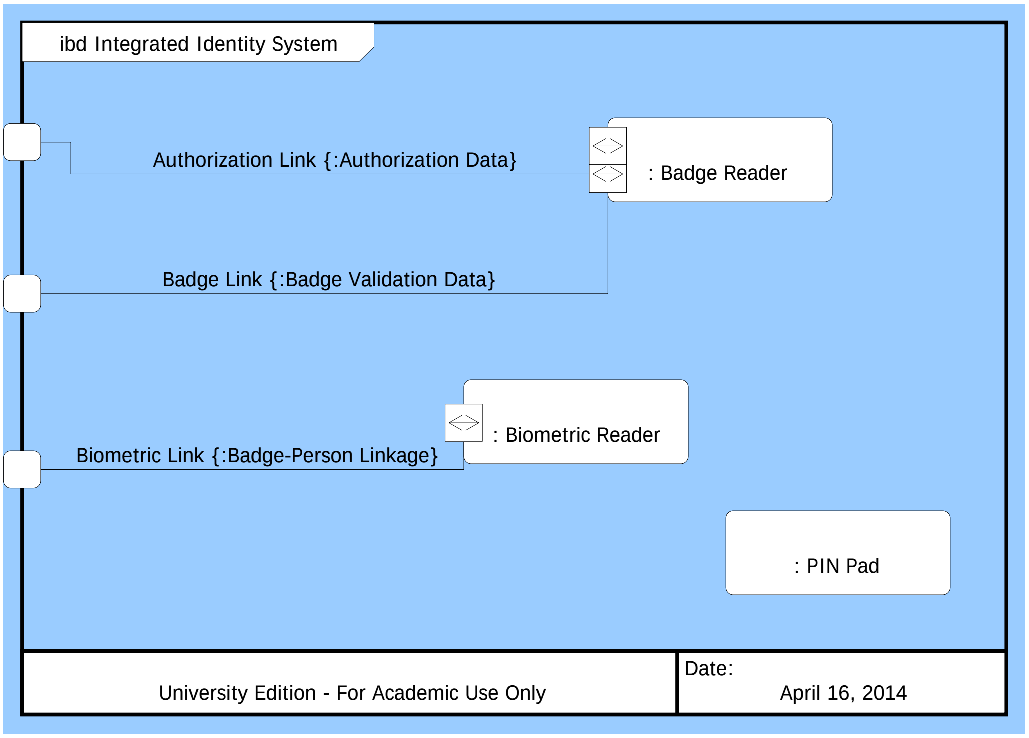

ibd Integrated Identity System
Authorization Link {:Authorization Data}
: Badge Reader
Badge Link {:Badge Validation Data}
: Biometric Reader
Biometric Link {:Badge-Person Linkage}
: PIN Pad
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 46. Identity Validation Interfaces

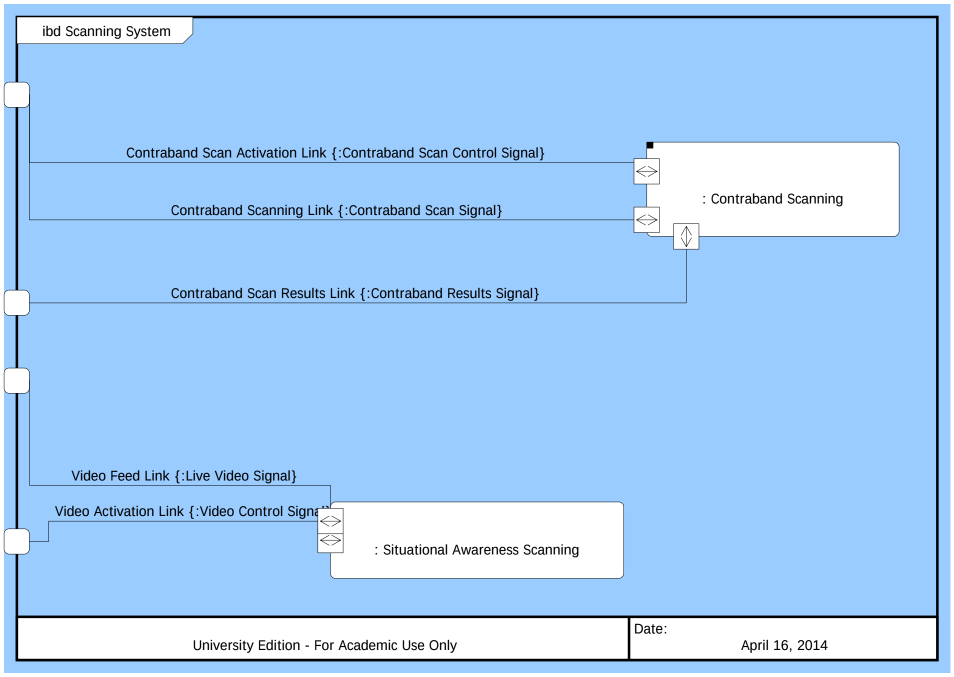

ibd Scanning System
Contraband Scan Activation Link {:Contraband Scan Control Signal}
: Contraband Scanning
Contraband Scanning Link {:Contraband Scan Signal}
Contraband Scan Results Link {:Contraband Results Signal}
Video Feed Link {:Live Video Signal}
Video Activation Link {:Video Control Signa
: Situational Awareness Scanning
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 47. Contraband Scanning Interfaces

In addition to transferring information for the ARAECS operators to grant authorized access, the system components need a method of control and activation for their use.

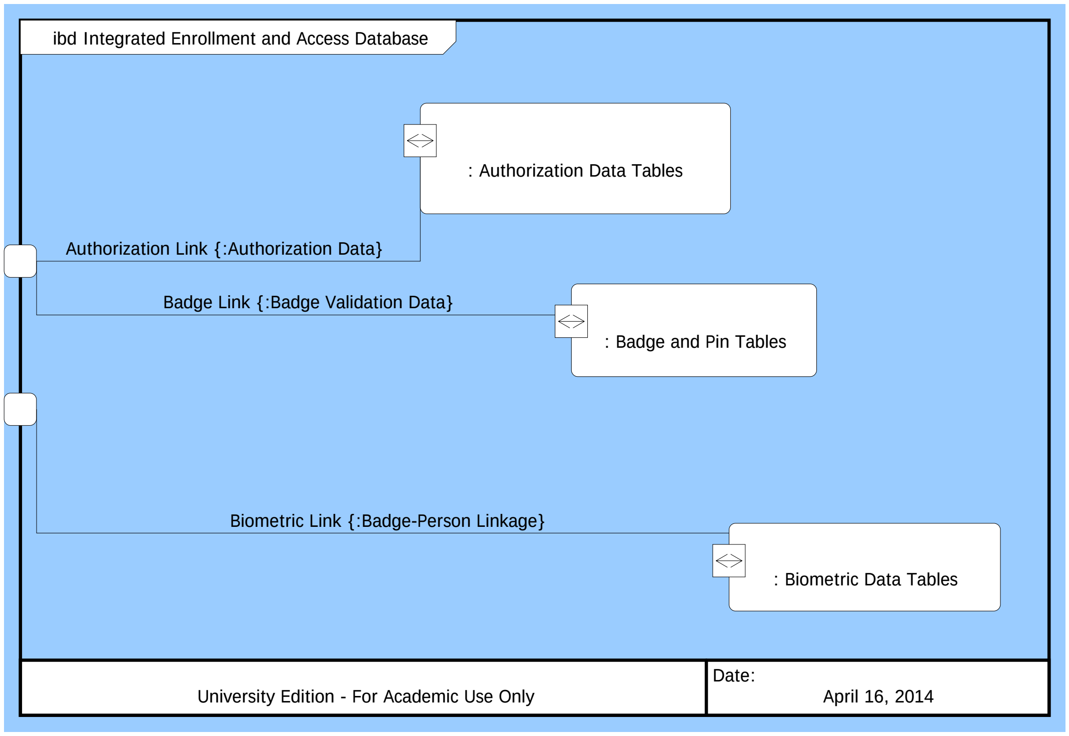

ibd Integrated Enrollment and Access Database
: Authorization Data Tables
Authorization Link {:Authorization Data}
Badge Link {:Badge Validation Data}
: Badge and Pin Tables
Biometric Link {:Badge-Person Linkage}
: Biometric Data Tables
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 48. Decomposition of Identity Validation Interfaces

The enrollment system is identified as an external system to ARAECS, but the details of the enrollment systems data allocation and data flow must be known to ARAECS so that the appropriate linkages can be implemented to pull data specific to identity, biometrics, and PIN.

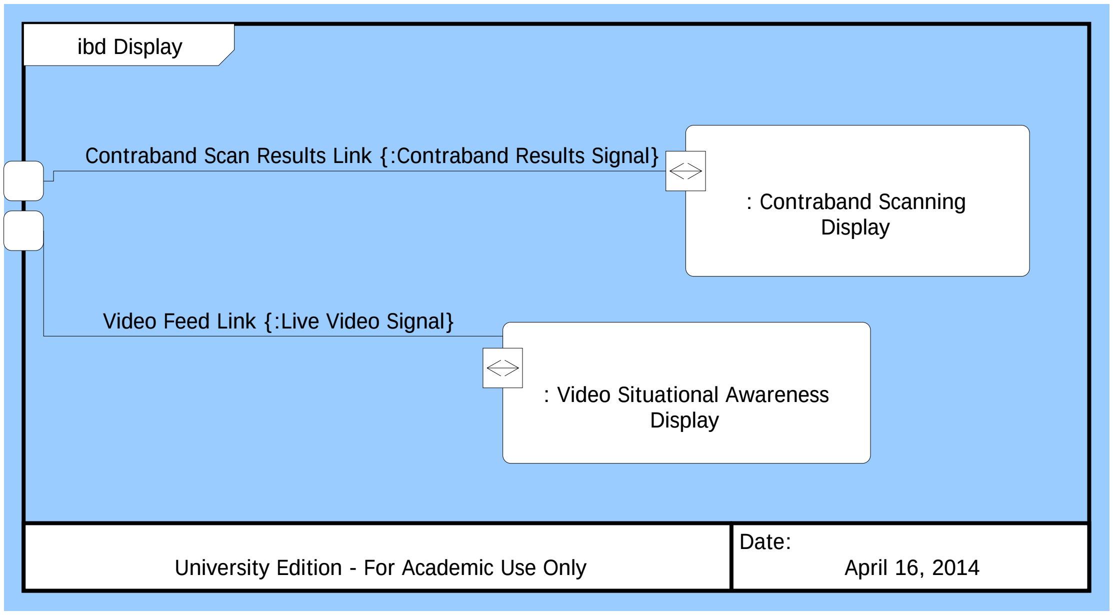

ibd Display
Contraband Scan Results Link {:Contraband Results Signal}
: Contraband Scanning Display
Video Feed Link {:Live Video Signal}
: Video Situational Awareness Display
University Edition - For Academic Use Only
Date:
April 16, 2014

Figure 49. Decomposition of Contraband Scanning Interfaces

9. System Performance Parameters Matrix

The System Performance Parameters Matrix is a compilation of the technical Measures of Performance that were derived from the Performance Modeling in ExtendSim8. They reflect the values used for the Hybrid-B Variant. These are not intended to be identified as “contractual-ready” threshold requirements, but rather the assumptions used to project a relative level of system performance.

As part of the detailed design process, systems engineers can identify particular cost-performance thresholds and perform parametric analysis around these values in order to identify potential efficiencies and cost savings. The obvious potential for commercial, rather than purpose built, technology must be considered. Additionally, conceptual design did not consider the use of system suitability, e.g., availability and maintainability, in the analysis. Further work can identify areas in which high performance but low availability may provide equivalent performance for a lower performing system that has higher availability.

Measure of Performance	Required Capability Value
Rate for Detailed Search Upon Entry	All personnel not prescreened + 5% of prescreened personnel
Rate for Detailed Search Upon Exit	Only escorted individuals require a detailed search
Pd for Contraband with a Detailed Search	0.95
Pd for Contraband with a Cursory Search	0.01
Delay for a Detailed Search (s)	120
Delay for a Cursory Search (s)	0.1
Pd to Detect an Unauthorized Badge	0.99
Pd to Detect an Unauthorized Individual	0.99
Pd to Detect Duress	0.99
Combined Delay to Conduct Badge Check, Verify Credentials, and Detect Duress (s)	12
Pd to Detect Contraband in a Vehicle	0.40
Delay to Conduct a Detailed Search of a Vehicle (s)	240

Table 14. System Performance Parameters

F. INTEGRATION

This project uses an integration process to systematically assemble lower-level system elements into successively higher-level system elements, iteratively with verification until the system itself emerges. Integration is essential to increasing system maturity, reducing risk, and preparing the system for transition to the stakeholder(s). Integration activities support an interface management process by verifying that accurate and effective interface specifications are documented. In parallel, the verification methods for each integration level are developed and included in the allocated baseline.

The successive integration phases follow a defined sequence and lead to the final product ready for verification and validation.

The Dual Vee entity models provide flexibility for variable product-line design. The initial problem statement incorporates two facilities that require enhanced system capability. Fulfillment of the prime directive may require separate solutions that integrate the unique command relationships and geographic differences at each site. Product line management through Dual Vee entities also allows the Navy future extensibility if detailed design is elected at future restricted area locations.

The team developed requirements and an executable architecture to represent the required operational capabilities. The team developed both of these products in Vitech's CORE. The completed CORE file is available upon request.

G. TEST AND EVALUATION

The ARAECS program requires verification and validation tests to show that the system architecture, simulation, and models fulfill the overall user requirements and fulfills the prime directive. The program and simulation assumptions will be validated through these tests. The test procedures and specific test details will not be part of this report. The test plans are divided into 5 categories:

(1) Requirements Testing. The program requirements are broken into two areas: Testable Requirements and Auditable Configuration Requirements. The Testable Requirements are, as the name suggests, requirements that can be verified through testing and evaluation. These requirements are the KPP thresholds and objectives and OMOE requirements. Verification of these requirements will be fulfilled with operational testing and field-testing. Auditable Configuration Requirements are requirements that relate to with physical and functional configuration. These requirements are found in various governing documents and are contained in the system specification document, Appendix I. Auditable Configuration Requirements will be verified through a configuration audit that includes functional architecture book to floor audit and physical architecture book to floor audit.

(2) Safety Testing. Safety testing is essential to verifying that the physical architecture is safe for use by both entrants and security personnel. Prior to safety testing, the safety team will perform a FMECA, Fault Tree, and Pareto analysis to determine and mitigate safety concerns. The safety crew will determine subsequent testing that will verify that the system will not cause a risk of physical harm unintentionally.

(3) User Interface Testing. This testing includes all testing associated with the human-machine interface, both the entrant as well as security personnel. Human factors are an essential consideration for the program. The user interface testing will include displays, heights and placement of hardware, ability of the system to work within the limits of human abilities, and verification of training. These tests can be done on a subsystem or component level. Full system level testing of these factors will be performed at Operational Testing.

(4) Operational Testing. Operational testing includes subsystem testing and system testing in a laboratory setting. Operational testing includes:

- Scaled blind tests resembling a single shift entering and leaving
- Subsystem Tests
    - Badge Reader
    - PIN Input Device
    - Personnel Scanner
    - Vehicle Scanner
    - Duress Code Input
    - Gates and other mechanisms
    - Personnel Badge Acquisition System Effectiveness Testing
- Verification of training of the security guards and support personnel
- Reliability, Availability, Maintainability (RAM) Tests
- Physical limit tests of the system (e.g., inputs are adjusted to saturation rates where feasible)
- System User Interface Testing
- Automated and Manual Entry Tests

Scaled blind tests will follow approximately the same modeling factor values as the simulation, namely:

- 5% entrants have contraband
- 0.01% acting under duress, with a minimum of 1
- 0.5% unauthorized entrants, with a minimum of 1
- 1% invalid badges
- 10% entrants require escorts
- 1% vehicle have contraband
- 40% entrants having a security clearance
- 5% of those entrants get security checks
- All other entrants have security checks

(5) Field Testing. The purpose of the field testing is to verify the system works under field conditions (i.e., in the intended operational environment). This test is the final test to validate the system will function to its requirements, fulfill the CONOPS, and verify the prime directive is achieved. Because this test is a demonstration and shakedown exercise, all testing performed in the operational testing phase will be performed in the field testing phase to verify that the security crew is trained and the process is proofed. Variations to the Operational Test methods with justification will be documented. This testing is the final testing before use in the field.

H. RISK MANAGEMENT

The following section describes the process by which the project team identified, assessed, and managed program risks.

1. Risk Overview

In accordance with Strategic Systems Programs Risk Management policy, SSPINST 5200.15, risks are maintained from program development through retirement in order to communicate, control and minimize risk to program cost, schedule and performance objectives.

2. Risk Identification

Risks are identified in the areas of cost, schedule, technical/performance, and affect on other systems. The emphasis in this report is on technical risks. Cost and schedule risks will be determined by the branch that actually administers the program. The project team will provide the risks developed as part of this report for consideration by the applicable branch into the branch risk register in accordance with the SSP Risk Flow Process shown in Figure 50. Then the risk will follow the respective branch policy for tracking and updating per the SSP Budget Call (SSP Notice 7100).

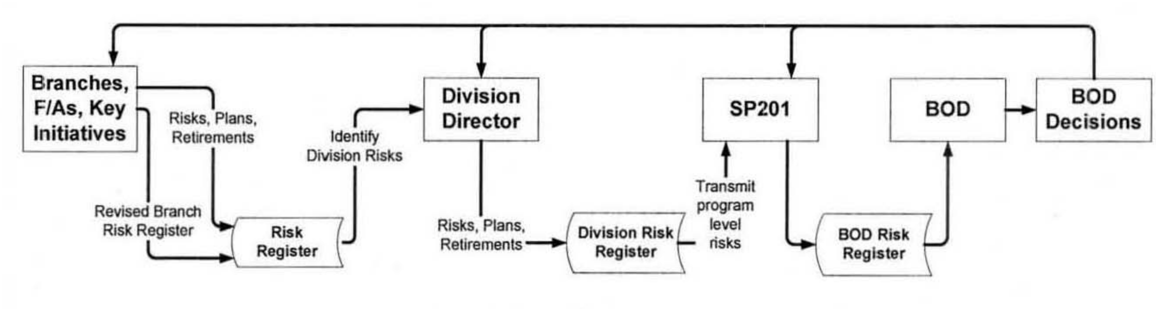
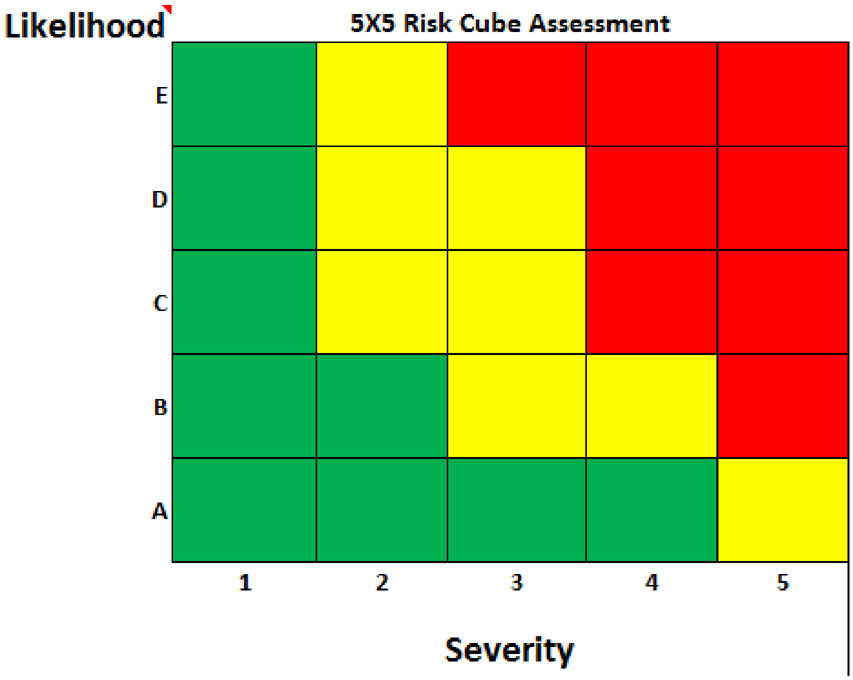

Branches, F/As, Key Initiatives
Risks, Plans, Retirements
Identify Division Risks
Division Director
SP201
BOD
BOD Decisions
Revised Branch Risk Register
Risk Register
Risks, Plans, Retirements
Division Risk Register
Transmit program level risks
BOD Risk Register

Figure 50. SSP Risk Flow Process

3. Risk Categorization

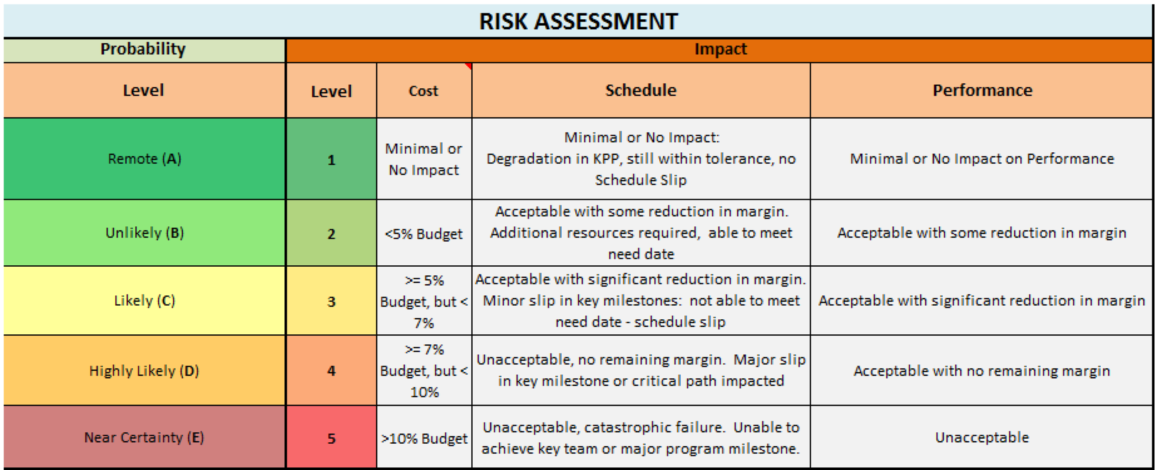
All areas identified as risks to the program, whether hardware, software, or people-ware, are assessed for likelihood of occurring and severity of the impact if the risk is realized. The 5x5 Risk Cube used is colored in accordance with SSP's risk tolerance shown in Figure 51 from SSP Notice 7100. This differs slightly from the standard DOD Risk Matrix.



Likelihood	1	2	3	4	5
E	🟩	🟨	🟥	🟥	🟥
D	🟩	🟨	🟨	🟥	🟥
C	🟩	🟨	🟨	🟥	🟥
B	🟩	🟩	🟨	🟨	🟥
A	🟩	🟩	🟩	🟩	🟨

Figure 51. SSP Risk Cube

The standards for classifying risk as low, medium or high are identified in the SSP Notice 7100 and are shown in Figure 52.



RISK ASSESSMENT				
Probability	Impact			
Level	Level	Cost	Schedule	Performance
Remote (A)	1	Minimal or No Impact	Minimal or No Impact: Degradation in KPP, still within tolerance, no Schedule Slip	Minimal or No Impact on Performance
Unlikely (B)	2	<5% Budget	Acceptable with some reduction in margin. Additional resources required, able to meet need date	Acceptable with some reduction in margin
Likely (C)	3	>= 5% Budget, but < 7%	Acceptable with significant reduction in margin. Minor slip in key milestones: not able to meet need date - schedule slip	Acceptable with significant reduction in margin
Highly Likely (D)	4	>= 7% Budget, but < 10%	Unacceptable, no remaining margin. Major slip in key milestone or critical path impacted	Acceptable with no remaining margin
Near Certainty (E)	5	>10% Budget	Unacceptable, catastrophic failure. Unable to achieve key team or major program milestone.	Unacceptable

Figure 52. SSP Risk Assessment

4. Technology Readiness Levels

As a part of technical/performance risk each technology needs to have its readiness level assessed based on the maturity of the respective technology. DOD Technology Readiness Assessment Guidance of April 2011 provides a table of technology readiness definitions shown below. The higher the TRL the more the technology has been tested and the closer it is to being ready to be used in an operational environment. The lower the TRL the more risk there is to being able to have the desired technology ready in time to meet program requirements

TRL	Definition	Description	Supporting Information
1	Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.	Publications or other references that outline the application being considered and that provide analysis to support the concept.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and comparisons were performed.
4	Component and/or breadboard validation in a laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and results from testing laboratory-scale breadboard(s). References to who did this work and when. Provides an estimate of how breadboard hardware and test results differ from expected system goals.
5	Component and/or breadboard validation in a relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity"	Results from testing laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the "relevant environment" differ from expected operational environment? How do test results

		laboratory integration of components.	compare with expectations? What problems, if any, were encountered? Was the breadboard system refined to more nearly match expected system goals?
6	System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology’s demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment	Results from laboratory testing of a proto-type system that is near desired con-figuration in terms of performance, weight, and volume. How did the test environment differ from operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7	System prototype demonstration in an operational environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an air-craft, in a vehicle, or in space).	Results from testing a prototype system in an operational environment. Who per-formed the tests? How did the test com-pare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
8	Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation (DT&E) of the system in its intended weapon system to deter-mine if it meets design specifications.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before finalizing the design?
9	Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions.	OT&E reports.

Table 15. Technology Readiness Definitions (DOD TRA 2011)

5. Risk Assessment

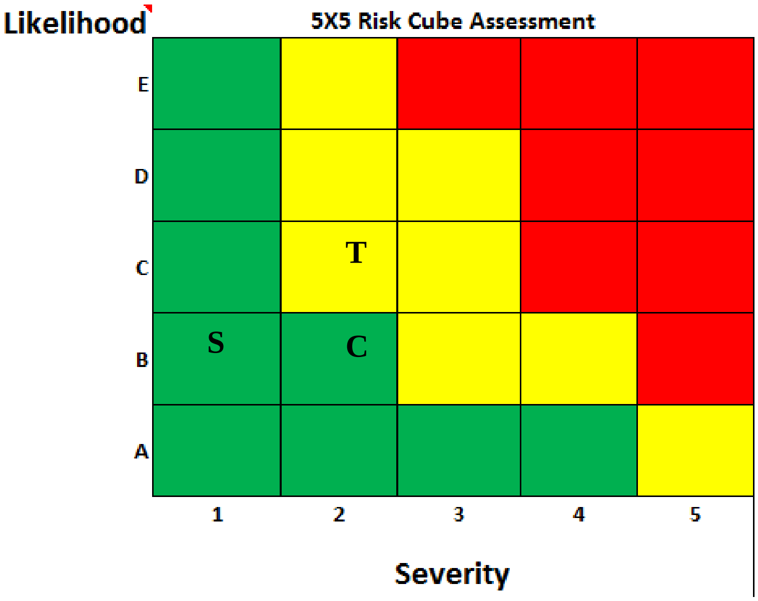


Figure 53. ARECS Risk Assessment

(1) Technology Risk Assessment (T). The overall system technical risk is assessed to be yellow because while there are examples of system candidate technologies already deployed in similar applications, there is inherent risk when combining these technologies into a system. Additionally, there are risks associated with “interfacing with other systems, so at this early phase of the development the likelihood of problems is ~50% with the severity assessed as “acceptable impacts to the performance with some reduction in margin.”

There are wide varieties of technologies that can be used to meet the requirements for identification and contraband detection. Each technology has been assessed using the Technology Readiness Level (TRL) described in Table 16. In the design phase the overall technology risk will need to be reassessed based on the technologies chosen. Of course, as time goes on the TRL may change as well. At the time of this report the subsystem technology risk assessments are based solely on the TRL and are shown in Table 16.

Technology Elements	**TRL**	**Comments**
Badge Reader	**9**	Technology is currently used in government office spaces to unlock doors
Smart Cards	**9**	Technology is currently used in DOD for identification
Millimeter Wave Detector	**9**	Technology is currently deployed by the TSA at airport screening locations for contraband detection
X-ray	**9**	Technology is currently deployed by U.S. Customs and Border Protection for contraband detection
Iris Recognition	**9**	Technology has been used effectively by police departments, sheriff’s offices, Federal Bureau of Investigation (FBI) and U.S. Army/Marines in Afghanistan and Iraq
Fingerprint Recognition	**9**	Technology has been used effectively by police departments, sheriff’s offices, Federal Bureau of Investigation (FBI) and U.S. Army/Marines in Afghanistan and Iraq
Facial Recognition	**5-6**	Great progress made over the past few years to develop software algorithms that automatically recognize individual’s features and effects the industry is still maturing.
Speech Recognition	**3-4**	Not ready for use within the scope of our project due to the varied environmental factors that will impact its usefulness as it is very sensitive to the environment.
Hand/Palm Print Recognition	**7**	Very similar to the fingerprint technology however it has been difficult to find reliable independent sources of data to validate the vendor’s claims of efficiency. The data available from commercial vendors is not sufficiently detailed to assess this technology any higher.
Vascular Recognition	**8-9**	Very difficult to forge, it is contactless, capable of many uses, is capable of 1:1 and 1: many matching, efficient and is cost effective. However, it has not gained as widespread acceptance compared to iris or fingerprint technology. It would not pose a serious risk if adopted.
Hand writing Recognition	**3**	Not ready for use within the scope of our project due to the varied environmental factors that will impact its usefulness.
Hand/Finger Geometry Recognition	**7**	Generally accepted systems. It is similar to fingerprint technology. Since fingerprints are seem to be the standard this may be more costly to implement within the scope of our project.

Table 16. Subsystem Technology Risk Assessment

(2) Schedule Risk Assessment (S). The overall system schedule risk is assessed to be green because the time to deploy requirement is not finalized so the likelihood is unlikely with a severity of minimal or no impact to the requirements.

(3) Cost Risk Assessment (C). The overall system cost risk is assessed to be green because the budget is not finalized. The likelihood is assessed to be unlikely to be exceeded. The severity is assessed to be within 5% of the overall budget due to the wide range of technologies available for the designers.

6. Tracking Risks

Risk tracking is imperative when it comes to risk mitigation. Risk can be a major disruption in any project and by tracking the risks and constantly keeping an eye on them will allow the project to flow smoothly. The team will maintain due diligence when it comes to risk tracking and risk mitigation. It is the responsibility of every group member to track and mitigate appropriately when it comes to independent and working group activities. It is the ultimate responsibility of the team leads to ensure that risk does not become a binding factor to the progression of the capstone project.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

Based on the analysis conducted, the team concluded that the Hybrid-B variant of the ARAECS provides the best solution for the identified capability need. The Hybrid-B variant includes three dedicated personnel entry lanes, four ECPs (including one dedicated to prescreened personnel), and it opens five additional lanes at each ECP during rush periods to further address wait times. It takes advantage of the DOD security clearance process to identify individuals who have previously established their trustworthiness to reduce the rate of detailed searches and thus improve overall efficiency. The team concluded that this was the best approach to balance the requirement for security with the requirement for reasonable security screening wait times. Other options were considered. However, none of the other variants achieved a satisfactory OMOE. Even the Super Variant had an unacceptably high OMOE, over four times greater than the Hybrid-B Variant.

The team concluded that the Hybrid-B architecture developed met the stakeholder requirements, though further work will be required to proceed to a detailed design. The functional architecture supports each of the four principal protocols: (1) the person and his badge must be validated, (2) the person must be authorized access to the specific restricted area, (3) a contraband search must be conducted, and (4) duress must be detected. The team determined that all of the required processes to accomplish the assigned mission were identified, these processes were allocated to functions, and the functions were allocated to objects. Therefore, the team concluded that this architecture could enable ARAECS to perform its required mission,

To summarize the process followed, the team started with an identification of the problem—the Navy needs an effective and efficient entry control system for restricted areas that house critical naval assets. The overall purpose of the project was to identify an ARAECS architecture that meets this requirement.

The first step was to determine the ARAECS requirements. These requirements were mostly obtained from DOD and Navy directives, but also elicited from stakeholders.

Then the team's methodology was to: (1) identify the required processes to satisfy the requirements, (2) allocate functions to the required processes, and (3) allocate objects to the required functions.

In order to model the ARAECS and ensure all of the main system requirements are met, the team identified four principle protocols: (1) the person and his badge must be validated, (2) the person must be authorized access to the specific restricted area, (3) a contraband search must be conducted, and (4) duress must be detected. Because a large work force must enter the restricted area in a reasonable amount of time, the team also had to consider how the ARAECS could be designed as efficiently as possible while still meeting security requirements.

ExtendSim8 was used to construct a model of ARAECS to allow the varying introduction of personnel and vehicles into queues to await individual entry to the restricted area. Model factors that influence performance were identified and then categorized according to the following: (1) uncontrollable factors (noise), (2) physical improvements, such as those that would require military construction, (3) technology improvements, and (4) human-based CONOPS improvements. The team chose to "bin" the factors as described above to inform possible trade space discussions. This was considered important because physical improvements require a large investment of resources, technology improvements are dependent on technological readiness and may not be immediately ready to implement, and CONOPS improvements are attractive because they are relatively easy to implement and normally do not require a large investment of resources. Initial results from the modeling and simulation conducted showed that the "Super Variant," which used best-case values for all factors, outperformed all others with the lowest wait times and security violations. However, even this variant had an unacceptably high level of security violations. When dealing with an SSBN environment, it is critical to minimize these violations which potentially have very serious consequences. These results led to two significant insights: (1) a workable solution must integrate aspects of CONOPS, technology, and physical improvements; and (2) without an integrated design, a system might achieve few violations or short waiting time, but not both.

To address this, since none of the initial variants adequately addressed the MOPs, the team searched for an alternative solution that performed as well as the "Super Variant," but without maximizing all performance factors (and thus resulting in a system with a very high cost) to achieve the desired responses for both precision and speed. Detailed searches give the best results for eliminating contraband but also take the most amount of time. As a result, the team determined that the best approach was to focus detailed searches on the least trusted personnel. The team selected the DOD security clearance process as an institutionalized system that allows a security force to compare relative trustworthiness as a result of background checks and command monitoring. Cleared personnel understand that certain violations put their clearance at risk and generally do not engage in those activities. However, as recent experience has shown, there is no absolute guarantee of trustworthiness—thus even cleared personnel require some random checks. The team thus determined that the cleared personnel would be subject to a 5% rate of detailed searches.

Additional modeling and simulation was then conducted using what the team termed the "Hybrid" approach. The Hybrid-B variant performed the best and was thus selected as the basis for the ARAECS architecture. The Hybrid-B variant includes three dedicated personnel entry lanes, four ECPs (including one dedicated to prescreened personnel), and it opens five additional lanes at each ECP during rush periods to further address wait times.

Using these modeling and simulation results, the team developed and described an architecture that aligns with the Hybrid-B variant. The ARAECS developed is an integrated entry control system that utilizes a combination of manpower, physical control features, and technology to control personnel, validate entry requirements, and screen for contraband. It physically interfaces with an existing boundary system (i.e., perimeter fence) and electronically interfaces with an enrollment database. It is highly robust with respect to the rate of unauthorized entry and personnel requiring escort. Its defining feature is the pre-screening of personnel through the use of the DOD security clearance background checks in order to allocate the majority of detailed searches to personnel that are relatively unknown and thus represent a higher risk.

There are areas for future research. The OMOE the team developed treated all security violations the same. Bringing plastic explosives into the restricted area is clearly more serious than a misspelled name on a badge. Additionally, specific weighting could be given to different types of contraband since automatic weapons represent a more significant threat than an unauthorized cellular phone. A better OMOE could be developed that takes these considerations into account. There are also opportunities for additional investigation to identify which candidate technologies should be incorporated into the system. More detailed analysis of candidate technologies could be performed to provide more precise values for technology factors that could then be fed into the model to see if additional insights could be gained.

Additionally, the architecture needs to be more fully developed. The architecture presented is nominal—and will require additional refinement to apply ARAECS to any specific location. This also has the potential to increase the security classification of the research since specific measures taken at specific locations are classified. Once the architecture is further refined, detailed cost analyses will be needed in order to make decisions about specific technologies and to inform possible trade space studies depending on the budget available.

APPENDIX A. OMOE DERIVATION

Overall Measure of Effectiveness Derivation and Sensitivity Analysis

The OMOE accommodates two Measures of Effectiveness: personnel wait time and the number of missed security violations:

$$OMOE = f(w_{t,}\, n_{sec})$$

Where w_t is the average personnel wait time in seconds and n_{sec} is the number of security violations (personnel that violate one of the four security protocols of authorized badge, authorized access, no contraband, and not under duress and granted access) over a 24 hour period.

The OMOE is constructed such that a lower value is a better performing system than a higher value since both a shorter wait time and fewer security violations are better.

The baseline measurement demonstrated the different scales of these two metrics: wait time was in tens of thousands of seconds and security violations were in the hundreds. Therefore, a simple summation would not provide an acceptable analytical response, e.g., a change in wait time of 900s would overwhelm a change of 50 security violations. Therefore, the OMOE was represented as a product of the two MOEs:

$$OMOE = w_t n_{sec}$$

An issue that arises from the use of a product is a wait time of zero will produce an OMOE of zero, and two candidate systems that have no wait time will not be able to differentiate if their security violations differ. Therefore, the factor in the OMOE calculation was set as a ratio that would approach 1.0 rather than 0 for a system without personnel delay. The value (5,000) used in the ratio was chosen since it was approximately half of the value of the Baseline System Variant’s personnel wait time of 10,656 s.

$$\frac{5000 + \ w_t}{5000}$$

Therefore, the OMOE becomes:

$$OMOE = \frac{5000 + w_t}{5000} n_{sec}$$

The next issue that arises is the clear distinction from the stakeholder surveys that reducing the number of security violations is more important than decreasing personnel wait time. The MOEs that comprise the OMOE must be weighted, and as the OMOE is a product, an exponential factor must be used for weighting:

$$OMOE = \frac{5000 + w_t}{5000} n_{sec}^{x}$$

where *x* is the weighting factor.

The team analyzed paired comparisons, assuming that a paired series of varying personnel wait times and security violations share the same OMOE and that iso-curve can be derived, which provides the exponential weighting factor. Therefore, for two wait times paired with security violations that equal the same OMOE *and* share the same constant exponential weighting factor for the security violations:

$$OMOE = \frac{5000 + w_{t1}}{5000} n_{sec1}^{x} = \frac{5000 + w_{t2}}{5000} n_{sec2}^{x}$$

For simplicity, the personnel wait time fraction for the derivation of *x* shall be stated as *y*.

$$y_n = \frac{5000 + w_{tn}}{5000}$$

Therefore,

$$y_1 n_{sec1}^{x} = y_2 n_{sec2}^{x}$$

Taking the natural logarithm of both sides yields

$$\ln y_1 + x \ln n_{sec1} = \ln y_2 + x \ln n_{sec2}$$

Solving for *x*,

$$x \ln n_{sec1} = \ln y_2 + x \ln n_{sec2} - \ln y_1$$

$$x \ln n_{sec1} - x \ln n_{sec2} = \ln y_2 - \ln y_1$$

$$x(\ln n_{sec1} - \ln n_{sec2}) = \ln y_2 - \ln y_1$$

$$x = \frac{\ln y_2 - \ln y_1}{\ln n_{sec1} - \ln n_{sec2}}$$

$$x = \frac{\ln \frac{y_2}{y_1}}{\ln \frac{n_{sec1}}{n_{sec2}}}$$

To address values used in the paired comparison, the team hypothesized a system that had a wait time of 0 s but 100 security violations. Qualitatively, and based upon the stakeholder surveys, the team concluded that a second system that had a wait time of 28,800s (an eight-hour day), but a 2/3 reduction in security violations to 33 had the same overall level of performance. Using these values:

$$y_1 = \frac{5000 + w_{t1}}{5000} = \frac{5000 + 0}{5000} = 1$$

$$y_2 = \frac{5000 + w_{t2}}{5000} = \frac{5000 + 28800}{5000} = 6.76$$

$$x = \frac{\ln \frac{y_2}{y_1}}{\ln \frac{n_{sec1}}{n_{sec2}}} = \frac{\ln \frac{6.76}{1}}{\ln \frac{100}{33}} = 1.72$$

Neither system performs acceptably, as no system should have a standard eight hour wait time, nor should allow 100 violations in the interest of speed. The purpose was to find two points on the same OMOE iso-curve to establish *x*.

Due to the somewhat subjective nature of this analysis, the team examined other potential paired comparisons: Note that due to the derived equation, the ratio of security violations improvement is relevant rather than the discrete number of violations from a single system.

- A system with a half hour wait time and ten security violations is equivalent to one with an hour wait time and a 10% reduction in violations.

- A system with no wait time and fifty violations is equivalent to one with a nearly 3 hour wait time but a 50% reduction in violations.
- A system with a five minute wait time and five security violations is equivalent to one with a nearly 3 hour wait time and a 40% reduction in violations.
- A system with approximately a half hour wait time and ten security violations is equivalent to one with a wait twice as long and a 10% reduction in violations.

Wait Time 1	Wait Time 2	Violations 1	Violations 2	y1	y2	x
0.00	28800.00	100.00	33.00	1.00	6.76	1.72
1800.00	3600.00	10.00	9.00	1.36	1.72	2.23
0.00	10000.00	50.00	25.00	1.00	3.00	1.58
300.00	10000.00	5.00	3.00	1.06	3.00	2.04
2000.00	4000.00	10.00	9.00	1.40	1.80	2.39

Table 17. Summary of Exponential Weighting Values Derived from Subjective Paired Comparisons

The exponential weighting factors ranged from 1.58 to 2.39, so a sensitivity analysis was conducted utilizing the baseline, CONOPS, physical, technology and super variants. As the OMOE is a relative, unit-less metric, the important summary is in the rank ordering of these systems. In addition to the ranged values computed through paired comparisons, the team added data points between 1.0 and 3.0 for comparison.

System Variant						
	Baseline	**CONOPS**	**Technology**	**Physical**	**Super**	*Exponential Weighting Factor*
OMOE	369	147	169	157	20	*1.0*
	595	207	269	257	27	*1.1*
	959	293	430	421	37	*1.2*
	1546	415	687	689	50	*1.3*
	2491	586	1098	1126	68	*1.4*
	4014	829	1753	1842	91	*1.5*
	6467	1173	2800	3014	123	*1.6*
	10421	1659	4472	4929	166	*1.7*
	43599	4691	18219	21566	407	*2.0*
	113201	9383	46474	57691	742	*2.2*
	182406	13269	74226	94358	1001	*2.3*
	5144662	150123	1967670	2954485	8149	*3.0*

Table 18. Sensitivity Analysis Summary of Varied Exponential Weighting Factors

Sensitivity Analysis Insights:

- Within the range of the calculated paired comparisons (1.58–2.39), the ordering of the systems’ performance remains unchanged (ordered from best performing to least):
  - Super
  - CONOPS
  - Technology

    - Physical
    - Baseline
- Utilizing 3.0 as a far range end point does not affect the rank ordering
- With an exponential value less than 1.3, to include an un-weighted value of x=1, the rank ordering is slightly adjusted, in that, the Physical and Technology variants swap places.

In conclusion, the original calculated exponential weighting value of 1.7 is used. It is roughly in the middle of the calculated range of possible values and the system performance ranking is not sensitive within a range that is inclusive of the calculated values. Therefore, the ARAECS OMOE is computed as:

$$OMOE = \frac{5000 + w_t}{5000} n_{sec}^{1.7}$$

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. TECHNOLOGY REPORT

A. EXISTING ENTRY ACCESS SYSTEM COMPARISON

This report examines existing entry access systems for comparison and analysis of alternatives. ARAECS (Advanced Restricted Area Entry Control System) is a new system that is intended to control the entry of personnel into a Level 3 restricted area. Existing entry control systems can be improved to gain both more efficient throughput and better security measures to ensure contraband does not enter the restricted area. The current system employs a “trusted agent” type of system where personnel are vetted prior to coming to the access point and given a badge. The proper security endorsements are then verified by a guard and random searches are exercised. Vehicles are searched when they are brought to the gate.

Research has shown that most entry access systems follow the trusted agent model. It is difficult to find descriptions of systems that have more stringent security than this in the open literature. The majority of the entry control systems that exist are software based and are used in conjunction with the Internet.

1. Summary of Existing Technologies Used for Entry Access Systems

a. Badge Reader

This technology uses a fob embedded in a picture ID card. When the correct card is presented to the reader, the reader sends a message to the control panel to unlock the door for entry. This is a type of key lock system where technology is used to replace the physical key and door lock. The holder of the card is responsible to ensure the risk of loss and theft is minimized. The user is required to report any loss or theft of the badge immediately. This is necessary because anyone in possession of the card can use it to gain access since a PIN or other code is not used in conjunction with this type of system. Even though the employee’s picture is printed on the card, anyone that has possession of the card can gain access. Employees and security personnel can detect an intrusion if they check for valid badges but this is not necessarily done on a routine basis. This type of system is typically used in an office environment.

b. Millimeter Wave Detector

This technology uses electromagnetic waves to detect hard objects that are hidden behind a person's clothing but it cannot penetrate the skin and is useful for detecting contraband hidden on a person. The system creates an image of a person as if their clothes were not on, creating a privacy concern. However, there is a capability for the system to filter out the detailed image and only identify areas of concern, thus reducing privacy concerns. The advantage of this technology is that a detailed search of the entrant can be made reasonable quickly without a physical hands-on search. This technology therefore offers quick throughput as well as a privacy capability. It does require personnel to operate, as well as hardware and software maintenance and support. There are no known health risks associated with this technology. This technology is mature and currently used by the TSA in airport screening.

A summary of the capability of a millimeter wave detector device is as follows:

- Screening time: 1.5 seconds (This is the time for the physical scan and does not include the time required for an operator to evaluate any areas of concern and conduct the required manual searches)
- Throughput: 200–300 people per hour
- No known health risks
- Detects items outside body cavity
- Could be configured to detect biometrics (facial recognition, height, etc)

The efficiency and speed of the system can be improved by advising personnel of the need to remove items from their person (wallets, keys, coins, etc.) which will minimize system detects and speed up the process. Since for the most part, the same personnel will be entering the facility day after day, it should be straightforward to train personnel in these areas.

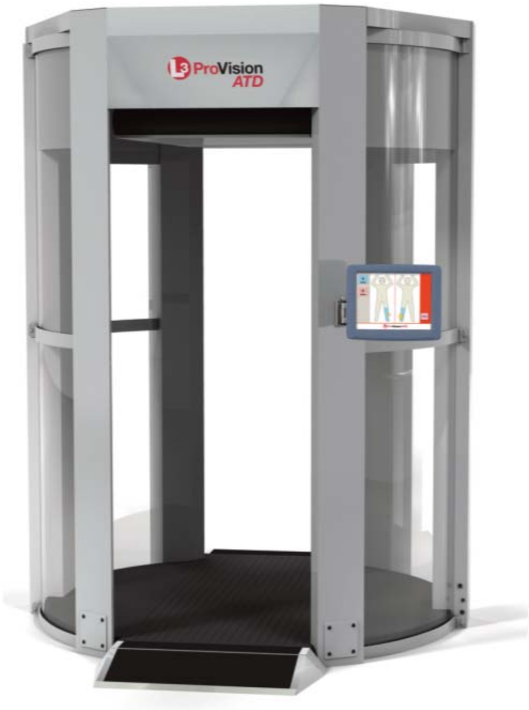


Figure 54. Millimeter Wave Detector (From L3 2013)

c. X-Ray

This technology allows detection of hidden objects using electromagnetic waves at a higher frequency then the millimeter wave detector. It is most useful in applications where humans are not exposed to the radiation due to the health risks involved. Shielding is required for security personnel. Current applications range from baggage screening to tractor-trailer screening. The capability of this technology is variable and depends on its application. This technology also has a capability to create an image that differentiates between organic and inorganic materials. This technology is mature and widely used in many applications such as baggage screening at airports. The screening times depend on the ability of the inspector to visually search each item. Larger items take more time because of the amount of volume that has to be inspected relative to the size of contraband that can be hidden. It is valid to assume the baggage screening size x-ray device works on average as fast as the millimeter wave detector. The ability of this device to detect contraband is highly dependent on the skill of the inspector reading the image.

This technology is best suited in screening vehicles that are being brought onto the restricted area. Various companies make x-ray machines that can scan tractor-trailers and are in use at border patrol checkpoints and customs screeners at ports.

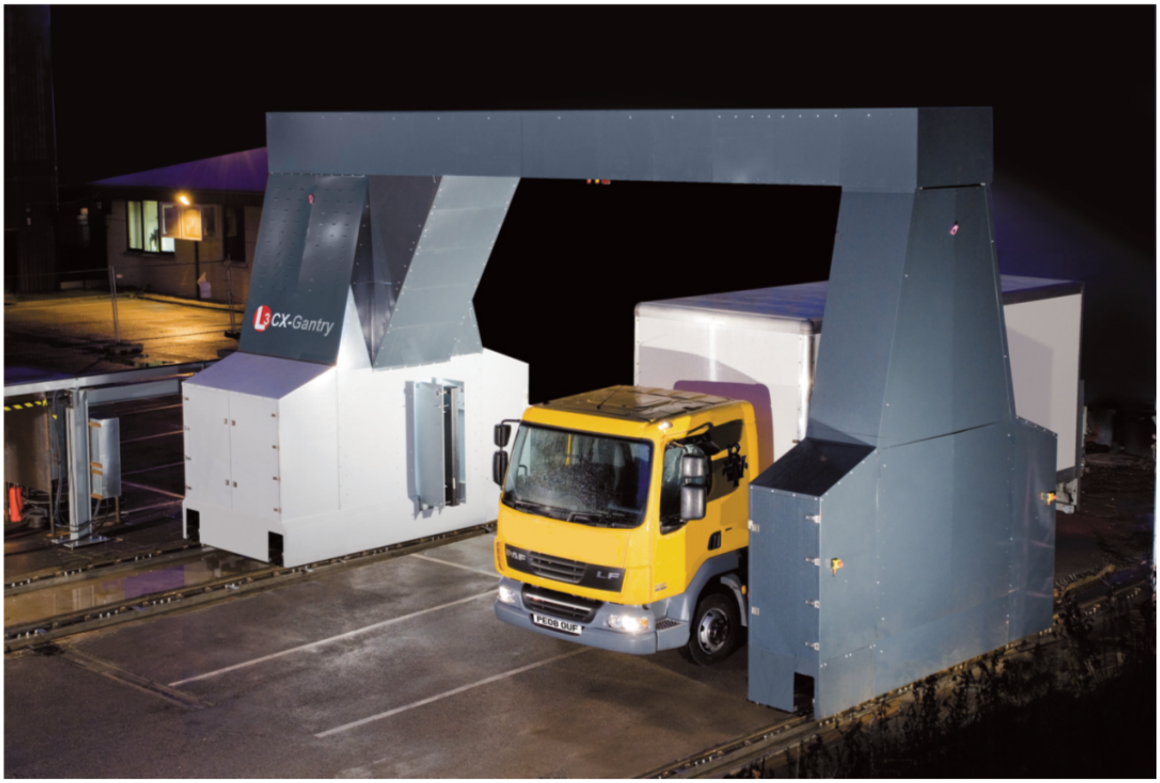


Figure 55. Gantry X-Ray System For Use on Tractor Trailers (From L3 2013)

d. CAC Card PKI Access

The CAC card is a multi-purpose identification card that allows both the user and the government to verify identity. With the implementation of biometric data in the CAC card, it could allow biometric verification of the holder. A more detailed assessment of this technology is made in Appendix II. Fingerprint data, an expected part of the biometric data in the CAC card, can be used by the organization to continuously check the FBI database for matches with suspects, in the unlikely case an employee or visitor recently committed a serious crime and did not notify the government.

2. Entry Access Systems

a. Trusted Agent

The trusted agent access system is the most prevalent in industry for entry access and is currently in use for restricted area access. It is established to allow ease of entry and relies heavily on the known worker integrity. The system recognizes individuals that have established that they can be trusted through a vetting process and gives them identification, keys, and/or passwords. They are then granted access by a guard or an automated door lock controlled by a card reader. Generally, random searches for contraband are performed, but not 100% of the trusted agents are searched on a daily basis (since they are assumed to be compliant with rules and regulations).

This type of system is similar to the local identity model used in software entry access systems, Figure 56. This system maintains a local user registry that other systems do not have access to and cannot change the local registry. If an external entity (e.g., an external computer through an emulator) wants to access the system, it has to acquire an identity for use with that system. It is simple and scalable. Each node, or computer accessing the system via a terminal, is associated with its local identity and access to computers is granted with a single sign on (only one username and password is required).[4]

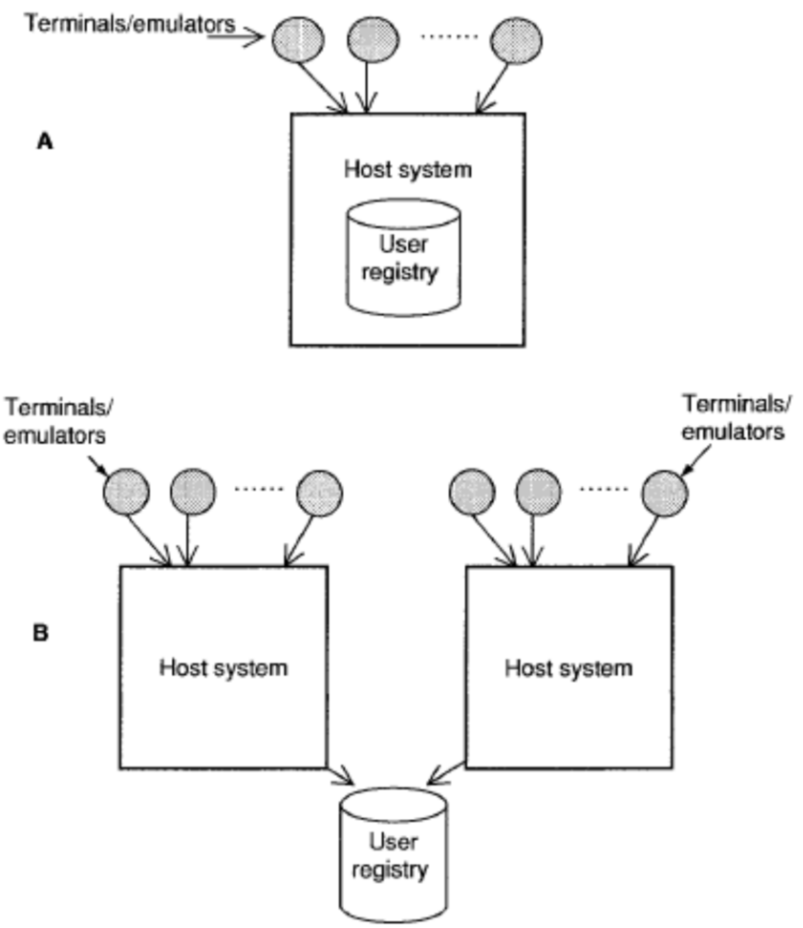


Figure 56. Local Identity Model for IT Systems (From Benantar 2006)

There are inherent risks involved in this model applied to an entry access system. First, this system doesn't ensure 100% positive measures are in place to prevent contraband from entering the restricted area (since not all entrants are subject to search—though they could be under heightened threat conditions). Second, it relies on the trusted agent's integrity, which can be compromised (although this risk cannot be totally eliminated, certain risk factors can be mitigated). Third, it doesn't prevent people that have recently experienced some kind of stress or been arrested or charged with a crime from entering—unless the system administrator has revoked their access within the system (which might rely on the individual self-reporting). Theoretically, under the trusted agent system, an entrant could be under severe mental stress within a day of requesting access and could gain entry, carrying in weapons or other contraband.

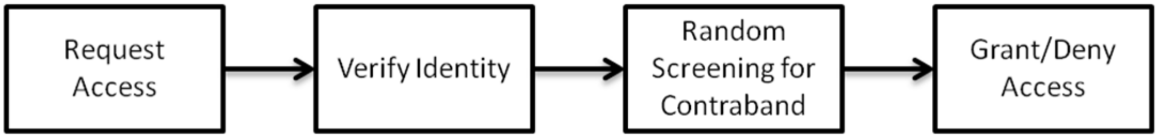


Figure 57. Functional Flow Block Diagram for Trusted Agent System

b. *Trusted Agent with 100% Search*

This system is like trusted agent but it includes a security detail that searches every entrant. It therefore achieves the level of security where vetted employees and visitors are verified to not have contraband. This system could provide more security than the simple trusted agent system but would have longer wait times and higher costs. This system could have built in biometric screening in that a human can recognize height, weight, and facial features of workers and visitors from their picture ID (CAC card and otherwise). The type of searches that a security detail would be able to perform is the same as a millimeter wave device. There would have to be a cost/benefit analysis to assess the life cycle cost and efficiency benefit of 100% manual searches vs. buying and maintaining automated hardware and software.

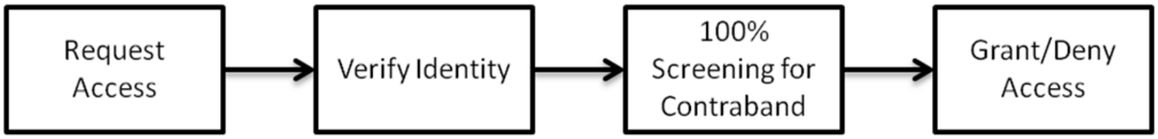


Figure 58. Functional Flow Block Diagram for Trusted Agent System With 100% Search

c. *Airport Screening*

The airport screening model is one of the most common entry access systems that many people experience. This system screens travelers from all over the world, some from countries that might not have friendly relationships with the U.S. There are hundreds of airports around the world, thousands of passenger jets in the air, and millions of travelers each year. For this system to be successful, most travelers are assumed to be carrying contraband and must be screened to the greatest extent permissible. Recently in the U.S., a system has been set up where pre-screened travelers can bypass some security measures (such as removing shoes), but still experience most of the screening requirements.

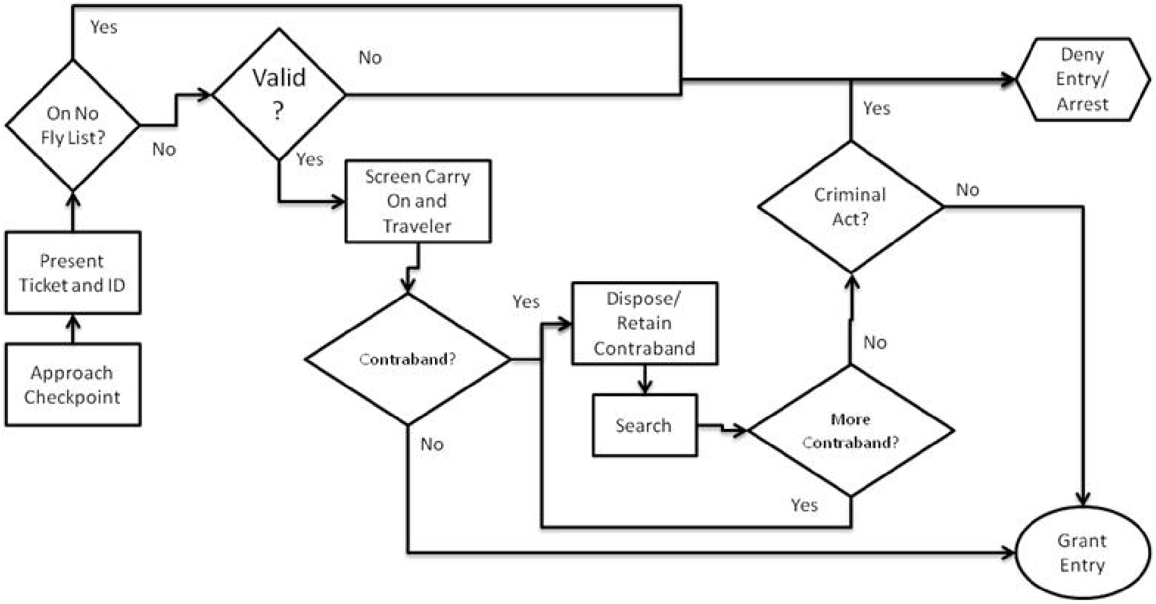


Figure 59. Airport Screening Logical Flow Diagram

Even though this is a tough problem, the system has been successful in preventing another 9/11-style terrorist attack via commercial air travel. It utilizes various modes of technology in conjunction with traditional means. The screener first verifies the identity of the individual is the same on the plane ticket, which is scanned into the system. This scan enters the travelers name into the computer to check against a no-fly list that is continuously updated by the TSA. At this stage, many different forms of identification are acceptable (passport, driver’s license, military identification, etc.) and no biometrics are checked—so there is a reasonable chance of success for someone using false identification to successfully pass through this stage. The traveler is then checked for contraband with an x-ray device (baggage) and a millimeter wave scanner (person). These two technologies replace the need to perform physical searches (unless something is triggered by the automated searches) and add an extra capability of detecting contraband hidden in solid objects. The TSA performs routine random physical searches as well as follow-on physical searches if contraband is found. Although random and follow-on searches aren't performed often, they are an effective means to ensuring the risk of contraband getting through is mitigated. Questions remain regarding this technology and its effectiveness. Does this technology search people faster, reduce manpower requirements, or does it add costs and work with software and hardware issues? Clearly in the airport screening system, the focus is more on finding contraband than ensuring only authorized personnel can pass through the checkpoint—since anyone who purchases an airline ticket is authorized.

There has been growing concern with the effectiveness of this system to block all threats. One risk with this system is airport employees, who are granted access through a trusted agent system different from that is used for air travelers. There are reported cases of employees gaining access through a badge reader and allowing otherwise unknown entrants to piggy-back in without scanning a badge. This type of breach relies heavily on the trusted agent, who has to understand and enforce the security policy. This type of concern is unlikely in the case of entering the restricted area because of attentive security at the checkpoint.

d. Computer Network System

Computer network systems are the prevalent and most visible access entry systems. This is because the Internet allows everyone access to all connected computers and security depends on each individual connected system. Hackers have been able to gain access to many of the most secure computer systems, which have fueled private companies and government research in more secure methods to controlling access. The ARAECS system might have connection to SWSNET, or other connection to the Internet that will allow the system to use fingerprint data to check against FBI lists, security clearance verification, or identity verification. Information assurance requirements will apply to these systems.

3. Conclusion

The airport system can be used as a model in some aspects for the ARAECS. Identity and clearance to enter can be verified against a local access registry using the CAC card, entering the correct PIN, and providing correct biometrics—providing even more assurance that only authorized personnel are allowed to enter. Another feature that can be established is to enable a duress code to be entered instead of the PIN, providing a means of communicating duress that is not apparent to a perpetrator. The access registry can be adjusted for regular workers or visitors. The person is checked for contraband, using a millimeter wave detector. The biometric data, specifically fingerprint, can be used to perform a search of FBI or other law enforcement database which provides a "continuous monitoring" capability in case an authorized person fails to self-report problems. This function allows the system to verify that the person did not recently become flagged for some incident, or otherwise placed on any watch lists.

The benefit to modeling the ARAECS on the airport screening system is that it reflects more positive control. It allows the ARAECS system team to understand the tradeoffs associated with using technology vs. manual screening.

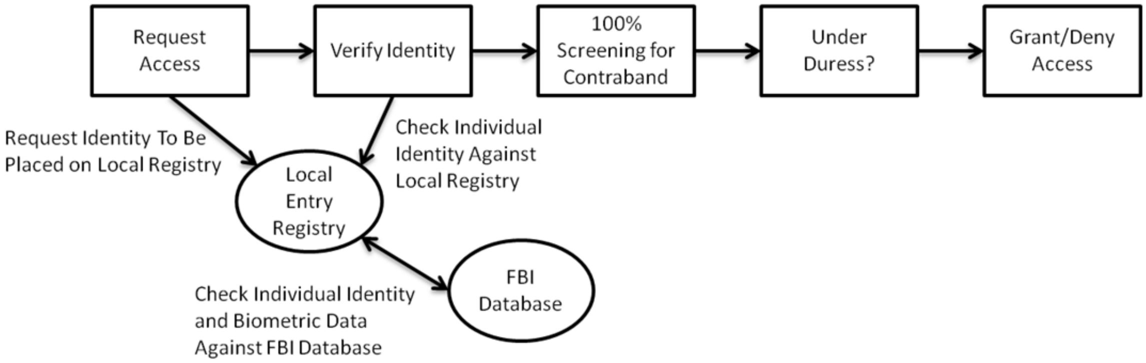

Request Access
Verify Identity
100% Screening for Contraband
Under Duress?
Grant/Deny Access
Request Identity To Be Placed on Local Registry
Check Individual Identity Against Local Registry
Local Entry Registry
FBI Database
Check Individual Identity and Biometric Data Against FBI Database

Figure 60. Enhanced Functional Flow Block Diagram Suggested for ARAECS System

B. BIOMETRICS

1. Introduction

There are three current levels of authentication: one level is something an individual has in his possession such as a token (key, card or badge). The most common form of token in DOD applications is the Common Access Cards (CAC). The CAC, a "smart" card about the size of a credit card, is the standard identification for active duty uniformed service personnel, Selected Reserve, DOD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DOD computer networks and systems (8521.01E 2008). Another level of authentication is a password. Passwords often must meet specified criteria in order to be a valid password. For example; one set of minimum requirements passwords must meet when they are created or changed is as follows (DoD 2011):

- <u>Must not</u> contain significant portions of the user's account name or full name.
- <u>Must be</u> at least eight (8) characters in length.
- <u>Must be</u> memorized.
- <u>Must contain</u> at least one character from three of the following four categories:
    - Uppercase letters (A-Z).
    - Lowercase letters (a-z).
    - Numbers (base 10 digits 0—9).
    - Non-alphabetic characters (` ~ ! @ # (8521.01E 2008) (8521.01E, 2008) (8521.01E, 2008) (8521.01E, 2008) (8521.01E 2008)$ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /)

The final type of authentication and the focus of this section is Biometrics. "Biometrics" is a general term used to describe a characteristic or a process.

As a characteristic: Biometrics is a measurable biological (anatomical and physiological) or behavioral characteristic that can be used for automated recognition.

As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics (National Science and Technology Council 2006).

A typical biometric system is comprised of five integrated components. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps the information for comparison with the new biometric templates. A matching algorithm compares the new biometric template to one or more templates kept in storage. Finally, a decision process (either automated or human assisted) uses the results from the matching component to make a high level decision (8521.01E 2008).

a. Background

There are many types of biometric devices, but there are five types of biometrics security that are most commonly used. These special biometric devices can often be seen in movies and TV shows, but these types of biometric security devices can actually be found in the most mundane places. Biometrics is basically the recognition of human characteristics that are unique to each human, which can include facial recognition, fingerprints, voice recognition, retina scans, palm prints, and more. Identification solutions, both conventional and Biometrics or a combination of both, have two possible working scenarios: enrollment and recognition.

Enrollment: When a new user wants to be introduced into the system, an enrollment must take place. The objective is to get the user's biometric template. This template will represent the user and will be used in all the recognition processes.

Recognition: There are two recognition processes: verification and identification.

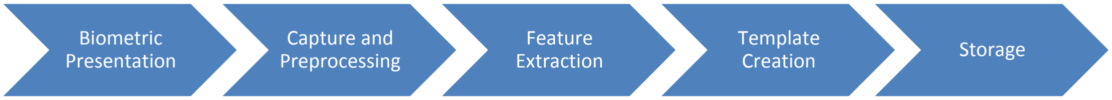


Figure 61. Authentication Process

b. Technology Readiness Assessment Overview

Many biometrics systems have evolved to a maturity level that offers viable alternatives to current technology without increasing the risk of overlooking a potential threat to restricted areas. The process typically used to assess the readiness level of any technology consists of a Technology Readiness Assessment (TRA) and as a result of the assessment a Technology Readiness Level (TRL) is assigned. The primary purpose of using a TRL for this project is to help mitigate the risks associated with adopting a "new" technology in the prevention of unauthorized access into restricted areas. An assessment was made of each technology using the Technology Readiness Level definitions, descriptions, supporting information and top level questions for determining the anticipated TRL (5000.2R 2002). A technology assessment maturity summary table is provided as Table 19 which defines each biometric modality as a critical technology element (CTE).

Critical Technology Elements	**Current TRL**
CTE 1—Iris Recognition	**9:** Current Iris technology has been used effectively by police departments, sheriff offices, Federal Bureau of Investigation (FBI) and U.S. Army/Marines.
CTE 2—Fingerprint Recognition	**9:** Current fingerprint technology has been used effectively by police departments, sheriff offices, Federal Bureau of Investigation (FBI) and U.S. Army/Marines.
CTE 3—Facial Recognition	**5-6:** Although there has been great progress made over the past few years to develop software algorithms that automatically recognize individual's features and effects the industry will continue to mature overtime.
CTE 4—Speech Recognition	**3-4:** This technology is not ready for use within the scope of our project due to the varied environmental factors that impact its usefulness.
CTE 5—Hand/Palm Print Recognition	**7:** This technology is very similar to the fingerprint technology; however it has been difficult to find reliable independent sources of data to validate the vendor's claims of efficiency.
CTE 6—Vascular Recognition	**8-9:** This technology is very difficult to forge, it's contactless, capable of many uses, is capable of 1:1 and 1: many matching, efficient and is cost effective. However, it has not gained widespread acceptance compared to Iris or fingerprint technology.

CTE 7—Hand writing Recognition	**3:** This technology is also not ready for use within the scope of our project due to the varied environmental factors that impact its usefulness.
CTE 8—Hand/Finger Geometry Recognition	**7:** Hand geometry recognitions systems are generally accepted systems. The type of system is no more or less accepted than fingerprint technology. Since fingerprints seem to be the standard this may be more costly to implement within the scope of our project.

Table 19. Technology Readiness Level Maturity Assessment

2. Biometric Modalities

a. Iris Recognition

(1) Overview. The Iris is the colored part of an individual’s eye. The concept of using the iris for recognition purposes dates back to 1936 (National Science and Technology Council 2006). The next major advancement appeared in the late 1980s with a patent issued in 1994 for algorithms that can perform iris recognition automatically. To obtain a good image of the iris, identification systems typically will illuminate the iris with a near infrared light, which most cameras can observe. However, this light is not detectable by, nor can it cause injury to humans. A common misconception is that iris recognition shines a laser on the eye to scan it. In reality, iris recognition simply takes an illuminated picture of the iris without causing any discomfort or injury to the individual.

(2) Cost. Iris and retinal scanning are both used to identify a person according to their unique pattern, but they tend to be far costlier and more complex than other biometric systems.

b. Fingerprint Recognition

(1) Overview. Fingerprint identification is one of the most well-known biometrics because of fingerprints uniqueness and consistency over time; fingerprints have been used for identification for over a century. Recently, fingerprint biometrics has become automated with the advancement in computing capabilities. Fingerprint identification is popular because of the intrinsic ease in acquisition, the many sources that are available for collection, and their established use and collection by law enforcement and immigration (National Science and Technology Council 2006).

(2) Concept. A fingerprint usually appears as a series of dark lines that represent the high peaking portion of the friction ridge skin and white space which correspond to the valleys between the ridges and the low shallow portion of the friction ridge skin. Fingerprint identification is based on the location and direction of the ridge endings and divisions along the ridge path.

(3) Fingerprint sensors. There are many different types of fingerprint sensors available commercially. The correct sensors for a particular system are dependent on that application's specific needs and requirements. Table 20 gives some of the sensors available and the applicable requirement that the sensor will work best (Bromba 2003).

Type of sensor currently best	**Requirement**
Capacitive line sensor	Low cost
Optical reflexive sensor	High level of development
Optical reflexive sensor	High image quality
Thermal/Capacitive line sensor	Small size
Optical transmissive sensor	High vandalism protection
Capacitive silicon sensor	High temperature span
Optical transmissive sensor	High forgery protection
Optical reflexive sensor	High ESD strength

Table 20. Fingerprint Sensor Type

(4) Cost. Fingerprint scanning is relatively inexpensive. The cheapest fingerprint scanners only scan the actual print, while costlier ones actually scan the presence of blood in the fingerprint, the size and shape of the thumb, and many other features. These costlier systems actually capture a 3D image of the fingerprint, thereby making it much more difficult for the fingerprint to be counterfeited.

c. Facial Biometrics

Humans often use faces to recognize individuals. Advancements in computing capability over the past few years now enable similar recognitions to be done automatically. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Face recognition can be used for both verification and identification (National Science and Technology Council 2006).

d. Speaker or Voice Recognition

(1) Overview. Speaker or voice recognition is a biometric modality that uses an individual's voice for recognition purposes (National Science and Technology Council 2006). Every person in the world has a unique voice pattern, even though the changes are slight and barely noticeable to the human ear. However, with special voice recognition software those tiny differences in each person's voice can be noted, tested, and authenticated to only allow access to the person that has the right tone, pitch, and volume of voice. It can be surprisingly effective at differentiating two people who have almost identical voice patterns.

(2) Approach. The physiological component of voice recognition is related to the shape of the individual's vocal tract which consists of an airway and the vocal cords where voice sounds come from (John D. Woodward 2003). There are two forms of speaker recognition: text dependent (constrained mode) and text independent (unconstrained mode). In a system using "text dependent" speech the individual will speak either a fixed password or prompted to say a specific phrase (e.g. "Please say the following numbers 33, 45, 88") (National Science and Technology Council 2006). A text independent system is more flexible since it does not require a specific password or phrase. This system is also appropriate where the individual may be unaware of the collection or unwilling to cooperate.

Speech samples are waveforms with time on the horizontal axis and loudness on the vertical axis as illustrated in Figure 62. The speaker recognition system analyzes the waveform and compares the sample against the database of waveform patterns to determine if there is a match.

Figure 62. Speech Recognition Waveform (From Shutterstock 2014)

Although this seems like a straightforward implementation, it does not come without problems. One of the major weaknesses of this form of verification/validation is that it is based on sound and is highly susceptible to environmental noise. This can cause problems when a user has enrolled in a quiet room and then attempts to enter the restricted area in a noisy environment. This might be the case in a noisy guardhouse or when a vehicle attempts to pass through a busy gate. For this reason, this biometric is probably not suitable for the ARAECS.

e. Hand (Palm) Print Patterns

(1) Overview. Palm print recognition implements many of the same matching characteristics as fingerprint recognition. Both palm and finger biometrics are represented by the information presented in a friction ridge impression. Because fingerprints and palms have both uniqueness and permanence they have been used for a century as a trusted form of identification. However, the palm has been slower in becoming automated due the restrictions in computing capabilities and live-scan technologies (National Science and Technology Council 2006).

Palm recognition technology uses similar physiological features as fingerprint recognition technology. However, friction ridges do not always flow continuously (like a fingerprint) which results in ending ridges, dividing ridges, and dots. Palm recognition is designed to interpret the flow of the overall ridge to assign a classification and then extract the minutiae detail (major features) of a fingerprint. When a hand is placed on a scanner, there is a unique fingerprint pattern as well as a unique size and shape of the entire hand. Hand characteristics includes the width and length of the palm, the width and length of the fingers, the distance between each knuckle, and the depth of each of the lines in the palm. Because of the number of additional features, palm recognition is more complex than regular fingerprint scanning, and is therefore much more accurate with less chance of falsification (National Science and Technology Council 2006).

(2) Hardware Requirements. Capacitive sensor determines each pixel value based on the capacitance measured. Optical sensor uses prisms to detect the change in light reflectance related to the palm and thermal sensors require a swipe of a palm across a surface to measure the difference in temperature.

(3) Software. Palm recognition software scans the entire palm or segments it into smaller areas for analysis and matching or enrollment. Palm systems partition their databases based on the location of a friction ridge area. Furthermore, searching only this region of a palm database rather than the entire database is more efficient.

(4) Palm matching techniques. Minutiae based matching relies on the minutiae points described previously, specifically the location, direction and orientation of each point. Correlation based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridge based matching involves using pattern landmark features such as sweat pores, spatial attributes, and geometric characteristics of the ridges and /or local texture analysis. All of these are alternates to minutiae characteristic extraction matching.

f. Vascular Recognition

(1) Overview. Vascular pattern recognition is also known as vein pattern authentication. It is a fairly new biometric. Using near-infrared light, reflected or transmitted images of blood vessels of a hand or finger are derived and used for personal recognition. Researchers have determined that the vascular pattern of the human body is unique to each individual and does not change as the individual ages (National Science and Technology Council 2006). Advantages for this technology include: (1) it is very difficult to forge—vascular patterns are unique and blood needs to flow to register an image; (2) it is contactless - the vascular pattern scanner uses passive infrared technology to capture an individual's unique vascular pattern from below the surface of the skin on the back of their hand. This simple to use, very fast, hygienic and highly accurate solution allows for a unique personal template to be captured, encrypted, and then stored a variety of ways. A user's vascular patterns are matched against personalized ID cards/smart cards or against a database of many scanned patterns.

(2) Approach.

6. In Fujitsu's Palm Secure technology for biometrics, contact-less palm-vein sensing can be used to project a vein and hand contour image.

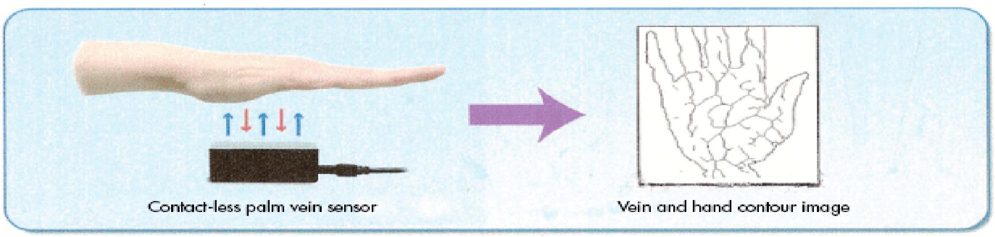


Figure 63. Palm Scanning Technology (From Allan 2008)

Near-infrared light generated from a bank of light emitting diodes (LEDs) penetrates the skin of the back of the hand. Due to the difference in light absorption of the blood vessels and other tissues the reflected light produces an image on the sensor. From the extracted image various feature data is stored as a template for later matching.

g. Handwriting Recognition

(1) Overview. Hand writing recognition technology uses the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase). It is not an image of the signature (common in locations where merchants are capturing signature for transaction authorizations). Dynamically captured data include:

- direction
- stroke
- pressure
- shape

The individual’s signature can be a reliable indicator of an individual’s identity (National Science and Technology Council 2006).

(2) Approach. Dynamic signature recognition uses multiple characteristics in the analysis of an individual’s handwriting. These characteristics vary in use and importance from vendor to vendor and are collected using contact sensitive devices such as tablets. Dynamic signature verification is a biometric that can be easily integrated into existing systems because of the availability and prevalence of signature digitizers and the public’s acceptance of this type of collection. On the downside however, current technology of signature recognition can only be used for verification purposes and has poor performance in some applications.

h. Hand/Finger Geometry Recognition

(1) Overview. One of the first successful commercial biometric products was a hand geometry system (National Science and Technology Council 2006). Typically a user enters a PIN code to claim an identity and then places his/her hand on the system, which takes a picture of the hand. Using mirrors, the picture shows the view of the hand from the top and side. Measurements are taken on the digits of the hand and compared to those collected at enrollment.

(2) Approach. The devices use a simple concept of measuring and recording the length, width, thickness and surface area of an individual's hand while guided on a plate. Hand geometry systems use a camera to capture a silhouette image of the hand. The image captures both the top surface of the hand and a side image that is captured using an angled mirror. Upon capture of the image 31,000 points are analyzed and 90 measurements are taken. The measurements range from the length of the fingers to the distance between the knuckles. This information is stored in nine bytes of data (an extremely low size) as a pattern for later matching (National Science and Technology Council 2006).

- Enrollment process:
  - Requires the capture of three sequential images of the hand
  - Creates a template of the users characteristics
- Submission process:
  - System recalls the template associated with the identity
  - Claimant places his/her hand on the plate
  - Systems capture an image and creates a verification template to compare the template developed upon enrollment
  - Similarity score is produced
  - Claimant is accepted or rejected based on the score

(3) Hardware devices. A charge-coupled device (CCD) is a light-sensitive integrated circuit that stores and displays the data for an image in such a way that each pixel (picture element) in the image is converted into an electrical charge, the intensity of which is related to a color in the color spectrum. A CCD in a digital camera improves resolution compared with older technologies. Some digital cameras produce images having more than one million pixels, yet sell for under $1,000. A good CCD can produce an image in extremely dim light, and its resolution does not deteriorate when the illumination intensity is low, as is the case with conventional cameras.

3. Conclusion

Some of these products will be far costlier than the others, as they feature technology that is much more complex. However, the amount spent on the various types of biometric devices will be directly proportionate to the level of security required. The more security needed, the more costly the device will be.

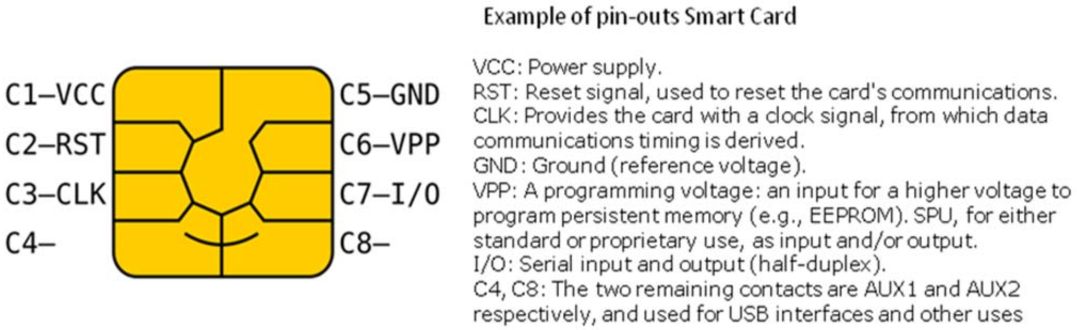
There are four key considerations discovered during this research. The first data point is enrollment time. Enrollment time is the time delay for an individual wishing access into a restricted area to present the particular biometric at the sensor and for the template to be created by the software and the template to be stored in the biometric database. The second key consideration is point template processing time. Template processing time is delay that can be realized during enrollment and again when the individual presents a biometric hours or days after initial enrollment. This is important because it is a delay that is required in the ARAECS. The third and fourth key considerations are FRR/FAR or False Rejection Rate and False Acceptance Rate. These measures are a measure of the risk of either falsely allowing an unauthorized individual into restricted spaces (FAR) or falsely rejecting an individual that is authorized into restricted spaces.

Overall, the additional security provided by the several modalities discussed within this report may not be cost effective to implement within the scope of ARAECS but the added security, the fast collection and error rates may prove valuable.

C. SMART CARDS AND BIOMETRIC PHYSICAL ACCESS CONTROL SYSTEMS

1. Introduction and Overview

A smart card is a plastic card with one or more computer chips on it. Other names for the same basic technology are integrated circuit card or chip card. These terms refer to any wallet-sized card supporting an embedded computer chip. These cards resemble credit cards in size and shape, but the inside is completely different. A normal credit card is a simple piece of plastic; smart cards have a microprocessor inside. This microprocessor is under a gold contact pad, as shown in Figure 64, accessible via one face of the card. This microprocessor gives the card enhanced functionality in such areas as data authentication, data storage and application processing (Smart Card 2014) (HowStuffWorks 2014). This is why smart cards are generally known for their ability to provide high end security features as opposed to massive data storage capabilities. Also, smart cards provide authentication and security systems and the benefit of portable and secure storage of valuable data (CardLogix 2010).



Example of pin-outs Smart Card

VCC: Power supply.
RST: Reset signal, used to reset the card's communications.
CLK: Provides the card with a clock signal, from which data communications timing is derived.
GND: Ground (reference voltage).
VPP: A programming voltage: an input for a higher voltage to program persistent memory (e.g., EEPROM). SPU, for either standard or proprietary use, as input and/or output.
I/O: Serial input and output (half-duplex).
C4, C8: The two remaining contacts are AUX1 and AUX2 respectively, and used for USB interfaces and other uses

Figure 64. Smart Card Pin Outs (From “Smart Card,” *Wikipedia*, June 15, 2014)

Most smart cards share several common physical characteristics. The ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters or in English standard units 3.370 by 2.125 inches. Another popular size is 25 by 15 millimeters or 0.984 by 0.591 inches. This is the size most commonly used in Subscriber Identity Module (SIM) cards. Both are 0.76 millimeters or 0.030 inches thick. As mentioned they can support and do normally contain a tamper-resistant security system, for example a secure crypto-processor and file system. Typically they are managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates (Smart Card 2014) (NIST 2003).

Smart cards interface with external services via two types of devices. Devices such as Automated Teller Machines, Document Insertion Processor Readers, and some types of Ticket Readers only read data from the card and do not write data to the card. Today the more common type are devices which both read data from and write data to the card; these are called smart card reader/writers (Smart Card 2014). The Advanced

Restricted Area Entry Control System (ARAECS) will employ devices which both write data to as well as read data from smart cards. Additionally, the ARAECS will utilize card reader/writers which are under continuous physical security protection. This protection will be maintained for all devices and equipment that constitute the ARAECS.

The United States Government maintains a 'General Services Administration Office of Government wide Policy' which further oversees a 'Smart Card Interoperability Advisory Board' (IAB). This advisory board publishes a 'Government Smart Card Handbook' which contains guidance with respect to Biometrics and Smart Cards.(GSA 2004) During the development of ARAECS this guidance will be followed in decisions pertaining to such issues as which types of chips and cards to use, smart card read/write devices, smart card interfaces, smart cards and building security, smart cards and IT security as it relates to logical access control, digital signatures, and most importantly biometrics and smart cards.

2. Current Application

One well-known application of smart card technology is the Department of Defense (DOD) Common Access Card (CAC) program. DOD is continuing to develop a comprehensive identity management system based on the CAC program. This will provide strong authentication for identity credentials and verification as well as strong identity binding to the back-end of the system utilizing biometric parameters (GSA 2004).

Additionally, there are many more smart card programs in use. The Deployment Personnel Accountability Readiness Tool (DPART) used by the United States Air Force was developed to integrate disparate, stove-piped personal deployment readiness information for Air Expeditionary Force (AEF) deployments via a distributed, web-based environment (GSA 2004). Lackland Air Force Base (AFB) uses a smart card system to issue cash to recruits arriving for training, done via a VISA cash card system. Recruits are issued a smart card as they arrive that confirms their arrival, completes their registration and disburses $250 as an initial pay advance (GSA 2004). In many European countries the health insurance and banking systems use smart cards extensively. In

Germany the health insurance system is using smart cards to identify persons as well as store the associated health records (Smart Card 2014).

Additionally, as part of a new program, the 25th Infantry Division in Hawaii was chosen for the field test of the Multi-Technology Automated Reader Card (MARC) card (GSA 2004). This card's applications include field medical documentation, mobility processing, manifesting, personnel accountability, health care and food service. The benefits of using the MARC card are demonstrated most clearly by the efficiency of deployment processing. A process which normally took a day or more is now reduced to a matter of hours and military personnel no longer waste time waiting in line. This functionality was integrated into the service member's common access cards (GSA 2004).

3. Personal Identity Verification

Personal Identity Verification (PIV) is the primary tool being utilized today in access control. The goal is to admit only authorized personnel to a particular location or region. Mechanisms used to verify identity using authentication factors are employed to achieve this goal. The act of relying on a specific number of authentication factors in an identity-based transaction represents the authentication method in use, see Figure 65.

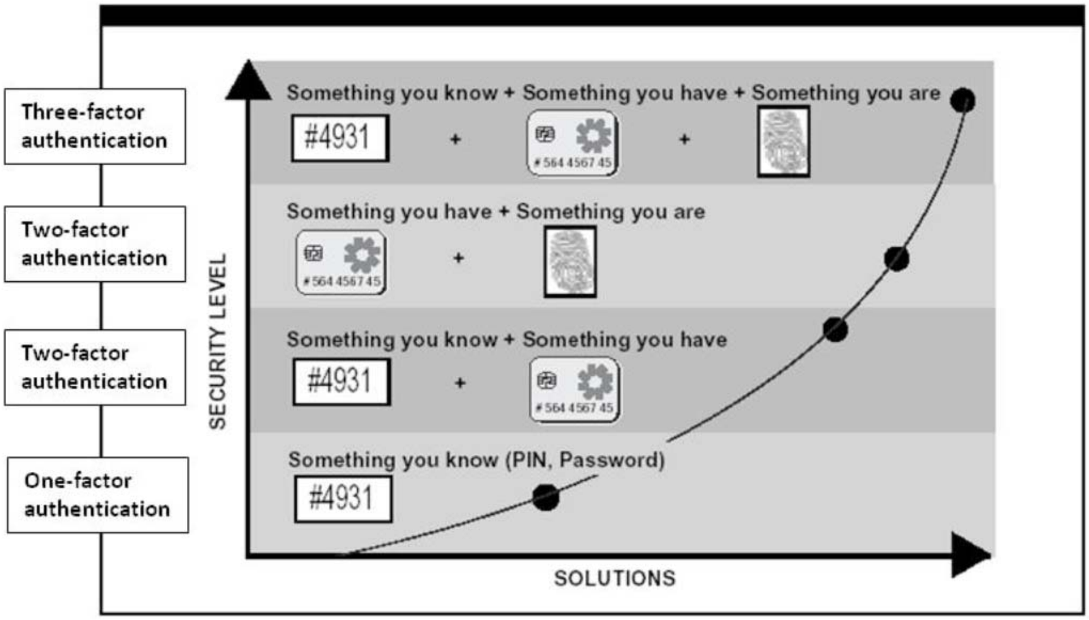

Three-factor authentication
Two-factor authentication
Two-factor authentication
One-factor authentication
SECURITY LEVEL
Something you know + Something you have + Something you are
#4931
+
#564 4567 45
+
Something you have + Something you are
#564 4567 45
+
Something you know + Something you have
#4931
+
#564 4567 45
Something you know (PIN, Password)
#4931
SOLUTIONS

Figure 65. Authentication Factors Scale (From SCA, 2011)

Verification of an individual’s identity is based on any one of but typically some combination of these factors:

- Item(s) presented upon demand such as a PIV card or a personal identification card
- Information possessed by the user provided upon demand such as an access code
- Inherent physical attributes of the user that can be demonstrated upon demand such as a unique fingerprint scan

The third factor is called biometric identification and is the newest member of the PIV family (SCA 2009).

4. Biometrics and Smart Cards

A biometric is a measurable physiological or behavioral trait of a living person, especially one that can be used to identify a person or verify a claimed identity. A biometric is uniquely bound to a person. A biometric can be used in conjunction with a password or a token (such as a smart card) to provide strong, two-factor authentication. Biometric systems have been commercially available since 1968; however, the use of biometrics has experienced significant growth only in recent years. In the future biometrics use is forecasted to increase in such areas as: time and attendance systems, customs and immigration, physical access control systems, ATMs and point-of-sale (POS) systems, and information system access control (SCA 2011) (CardLogix 2010).

There are many potential benefits of using Smart Cards in Biometric applications. With the improved acceptance and growing applications of smart cards, the cost of the cards is falling. Better operating systems and faster processors are reducing the read and write times associated with smart cards. Memory capacity and processor speed continue to increase. The move to multi-application cards is driven by ongoing enhancements in card capability such as increased memory as well as improved security. Smart cards can help centralize the identity verification process, that is to say they can eliminate the need for multiple cards by providing a dependable digital credential (GSA 2004).

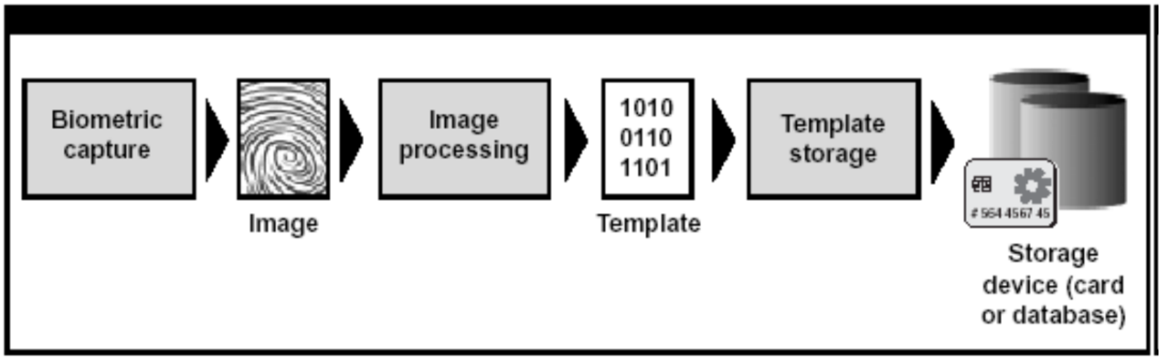


Figure 66. Example Enrollment Process (From SCA, 2011)

Although biometric technologies differ in what and how they measure, all biometric systems work in a similar way (see Figure 67). The subject submits a sample—that is, an identifiable, unprocessed image or recording of the physiological or behavioral biometric—via an acquisition device. This biometric is processed to extract information about distinctive features to create a trial template. The trial template is the equivalent of the user's "password." A trial template is compared against a reference template that was created from multiple images when the person enrolled in the biometric system (SCA 2011).

Biometric systems are not infallible. Biometric verification can fail as these systems do have a finite probability of error. They can attempt to match a subject's trial template with the wrong reference template. No two scans are ever identical; the match must be ascertained via stochastic constraints. These facts create a strong link between smart card capabilities and biometric systems needs. Depending on the biometric system, the role of the smart card can be quite varied.

There are two primary methodologies associated with the way smart cards can be utilized to verify biometric data. The first is match off-card where the enrolled template is initially loaded onto the smart card and then dispensed from the smart card via either contact or contactless interface. When requested by the external biometric system, the external equipment then compares a new live scan template of the biometric with the one being presented from the smart card (GSA, 2004). The second is match on-card where the reference template is stored in the smart card's secure memory. When a biometric match is requested, the external equipment submits a new live scan template to the smart card. The smart card then performs the matching operation within its secure processor. The results are then electronically communicated to the external equipment (GSA 2004).

Because the matching operation is performed internal to the smart card, match on-card is considered more secure. This method protects the initial reference template since it is maintained within the smart card and never transmitted off-card. Cardholder privacy is more securely maintained with this technique since the cardholder's biometric template information is not readable from the smart card. With this technique, the smart card must be microcontroller (as opposed to just memory) based and be capable of computing the one-to-one match (GSA 2004). The Advanced Restricted Area Entry Control System architecture will be determined by many parameters; however, the additional security features associated with match on-cards will be a consideration factor.

There are two primary types of biometrics: physiological and behavioral. A physiological biometric (also called physical biometric, static biometric) is a biometric based on data derived from measurement of a part of a person's anatomy. Examples of physiological biometrics include fingerprint, hand, face, iris and retina. A behavioral biometric (also called dynamic biometric) is a biometric based on data derived from measurements of an action performed by an individual. Behavioral biometrics are distinct in that they incorporate time as an element or component of the metric. Examples of behavioral biometrics include voice and signature (SCA 2011).

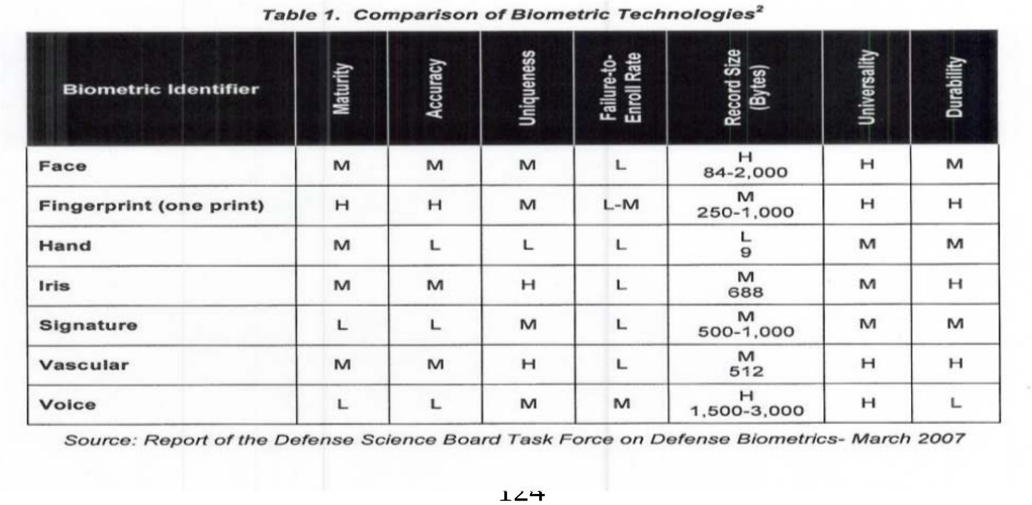


Table 1. Comparison of Biometric Technologies²

Biometric Identifier	Maturity	Accuracy	Uniqueness	Failure-to-Enroll Rate	Record Size (Bytes)	Universality	Durability
Face	M	M	M	L	H 84-2,000	H	M
Fingerprint (one print)	H	H	M	L-M	M 250-1,000	H	H
Hand	M	L	L	L	L 9	M	M
Iris	M	M	H	L	M 688	M	H
Signature	L	L	M	L	M 500-1,000	M	M
Vascular	M	M	H	L	M 512	H	H
Voice	L	L	M	M	H 1,500-3,000	H	L

Source: Report of the Defense Science Board Task Force on Defense Biometrics- March 2007

Table 21. Comparison of Biometric Technologies (From SCA 2011)

Table 21 provides additional features associated with each of the two types of biometrics. Physiological biometrics are unchanging (without significant physical injury) and unalterable (without significant duress). Biometrics associated with physiological traits are considered to be more invasive and individual privacy is an issue. Behavioral biometrics are considered less stable than their physiological counterparts because they can change more throughout the individual's life due to issues such as stress and sickness. For this reason, they are considered to be less useful in high security systems. Different types of biometrics that can be used with a smart identification card include: fingerprint, hand geometry, facial recognition, iris and retina scan, and voice and signature (GSA 2004).

The fingerprint is one of the most widely used biometrics in the government today. It has been estimated that the chance of two people having the same fingerprint is less than one in a hundred billion, even for identical twins (GSA 2004). Hand geometry systems use optical technology to map key geometrical features of hand topography (GSA 2004). Measurements include finger length, skin translucency, hand thickness, and palm shape. Facial recognition is based on comparing the characteristics of a live scan of a face against a stored template of facial characteristics (GSA 2004).

Two of the most fascinating areas for biometric scan potential are associated with the human eye. In the 1960s ophthalmologists proposed that the iris might be used as a kind of "optical fingerprint," based on clinical results that showed that every iris is unique and unchanging.   In addition, retina scan is the most accurate and reliable biometric technology. The patterns of the retinal blood vessels are measured at over 400 points to generate a 96-byte template. Retinal patterns, again even between identical twins, are unique. Both of these patterns do not change during the course of an individual's lifetime absent some disease or injury (GSA 2004).

As mentioned above behavioral biometrics also presents potential. Voice verification is possible because every person has a unique set of voice characteristics and speech patterns. Voice verification extracts specific and unique features from a person's speech, such as pitch, tone, cadence, harmonic level and vibrations in the larynx, and stores and uses them to differentiate that person's voice from other voices (GSA 2004).

Signature identification systems analyze two different areas of a person’s signature: the specific features of the signature itself (the visual image) and the specific features of the process of signing (GSA 2004).

All organizations which utilize a biometric based system, smart card or otherwise, will deal with privacy and suitability concerns. These include fears about the organization’s ability to search through an individual’s private records and to track the person’s actual movements. There could also be concerns about biometric scanning devices such as iris and retina scanners which can, if programmed, function as cameras. There could be concerns about biometric scanning devices such as voice and speech recognition devices which may also function as microphones. Smart card- based systems can alleviate these concerns since the biometric information can be securely stored on the card (GSA 2004).

In terms of suitability it is important to remember that approximately 2 percent of the general public does not have the feature required for mapping any one specific biometric. Users who are mute cannot use voice systems. Users lacking fingers or hands from congenital disease, surgery or injury cannot use fingerprint or hand systems. Therefore, any organization that employs a biometric system will probably require a secondary system, not necessarily using another biometric. This secondary system must be at least as secure as the primary system (GSA 2004).

One way to approach this problem is by using ‘multiple biometric modalities’ which simply utilize a combination of more than one biometric feature in the same system. More than one measurement can be mathematically “fused” to provide a unique representative data set. This option then creates the possibility of allowing a limited number of individuals with extenuating circumstances to, via appropriate deviation; submit only one required biometric sample (SCA 2011).

a. Supporting Technology – Smart Card Read/Write Devices and Host Computers

Smart cards utilize devices called reader/writers as the required link between the card, the host computer, and the associated software. Smart card reader/writers can simply function as signal throughput devices with all processing and application delivery being performed by the host computer—a transparent reader/writer based system. Or the reader/writers can be standalone devices; although they are never standalone devices in the strictest sense. A standalone system still requires a host computer. The read/write device contains the firmware required to function as an interface between the smart card and the host computer. In a standalone system - the host does not communicate directly with the smart card; the host is limited to communication with the read/write device which then interfaces with the smart card. On the other hand, transparent read/write devices have no internal logic - except for signal conditioning capability between the host and the card. A host drives the reader/writer and the card. The associated software application accommodates both the reader/writer as well as the smart card's communication requirements (GSA 2004).

b. Contact and Contactless Smart Cards

The two types of smart card chip interfaces used today are called 'contact' and 'contactless'. The names indicate the way data is read from and written to the associated card and the way in which electrical power is supplied. Single cards may support contact and contactless interfaces. This can be accomplished in one of two ways: a card can support two separate chips or a dual-interface chip. As the name would imply contact based smart cards are physically placed or inserted into the associated read/write device. Contactless smart cards are placed in proximity to the read/write device, generally within 10 centimeters (GSA 2004). Due to security considerations the ARAECS will consider contact based smart card systems to be the primary candidate for implementation.

In both types of interfaces read-only memory contains the chip's operating system. Both types of interfaces also utilize FRAM (ferroelectric RAM). FRAM offers the advantage of reading data thousands of times faster at far lower voltage than other non-volatile memory devices. All smart card secure microcontrollers have internal functionality such as environmental sensors (e.g., voltage, frequency, and temperature), at least one serial communications port, a random number generator, and timers (GSA 2004).

5. Cost Factor and Risk Consideration

The applications selected by any particular agency will have a strong influence on cost. In developing smart card systems participating parties must strike a balance between system cost and desired functionality. The cost of the chip card may vary substantially, depending on the number of chips per card, size, and capabilities of the chip(s). While it may make sense to use contactless chips for physical access control at ECPs because this substantially increases throughput for perimeter control, it may not be feasible from a cost perspective. In addition to the cost associated with smart cards and their associated readers, there are many other start-up as well as ongoing costs to consider (GSA 2004).

Some of the costs associated with design and development are detailed system design and review, hardware and software development, system demonstration and acceptance testing, manuals and training materials, and independent validation and verification. Additional implementation costs can include hardware, switching agreements, licenses, software, telecommunication lines, and terminal deployment. Once the system is in place ongoing costs such as annual help desk support for system data or program issues, and user updates and training must be considered (GSA 2004).

a. Other Considerations for Smart Card Based Access Control Systems

The National Institute of Standards and Technology (NIST) has developed a document entitled ‘A Recommendation for the Use of PIV Credentials in Physical Access Control Systems’ otherwise known as SP 800–116. This document recommends that a comprehensive security risk assessment should be used by facility security managers in order to define the necessary authentication mechanisms required to respond to various threat levels and types in different areas of the facility in question (SCA 2009).

The location of card readers at points which are susceptible to heavy weather and or humidity conditions such as area perimeter gates or boat docks should be avoided. This may preclude the use of contact smart card readers because moisture or airborne contaminants present a potential hazard to the internal reader electronics. When card readers must be placed outside, they should be placed in a temperature and humidity-controlled enclosed structure (SCA 2009).

As stated above, SP 800–116 is not a requirements document for DOD applications. However, Joint Air Force–Army–Navy (JAFAN) Manual 6/9; the Director of Central Intelligence Directive No. 6/9 (DCID 6/9); and OPNAV INSTRUCTION 5530.14d do provide guidance. These documents set requirements for the maximum probability of an unauthorized entry as well as authorized entry denial (SCA 2009). While a comprehensive overview of all systems available today is beyond the scope of this paper; the system selected for ARAECS must meet applicable requirements.

Regulations also mandate that Physical Area Control Systems administrative control panels be located within the protected area in question. There are also specific requirements applicable to communication lines, cryptographic protection and shielding (SCA 2009).

b. Match Speed and Data Transfer Rate

Current smart card data transfer rates are well within the range needed to support biometric applications; a transaction can be completed in one or two seconds (SCA 2011). Today, providers of high-precision biometric fingerprint, face, iris, palm-print and voice identification algorithms can utilize this data as fast as it can be provided. High-end systems boast facial recognition matching speeds of up to 100 million templates per second making it possible to match faces as fast as fingerprints. Additionally, as many as 200 million irises per second can be matched with modern biometric systems (NEUROTEC 2014). With the smart card based biometric systems available, match speed and data transfer rate should not present a limiting constraint to ARAECS functionality.

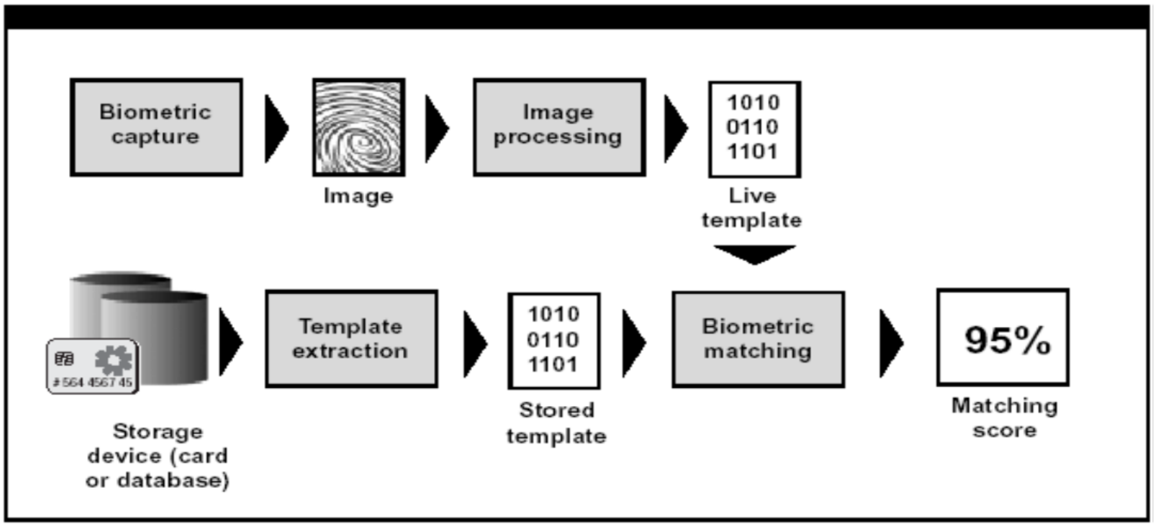


Figure 67. Example Matching Process (From SCA 2011)

c. Technology Readiness Assessment

The government has accepted smart cards technology. The technology is being readily and aggressively implemented. Millions of smart cards have now been issued to government employees. Smart cards are being used in numerous government agencies and at every level of functionality. With respect to the smart cards themselves and associated system elements, actual similar systems have been proven through successful mission operations (DOI 2009).

d. Conclusions and Recommendations

Highly dependable identity recognition and identity management systems are very important to government organizations and any other entity that must correctly verify the identities of a wide variety of people such as: employees, contractors, emergency response officials and visitors (SCA 2010).

Smart cards are designed and manufactured for security and are much less vulnerable to such attacks as malware, forgery and other efforts to extract or alter information. Smart card technology can be used to make identity credentials more secure. The global ePassport program is used in more than 100 countries. The United States Government has issued a Personal Identity Verification (PIV) card to all federal employees. This card is used for physical access to buildings as well as access to networks and computers. Government agencies and many other businesses use smart card identity cards and tokens for internal technology security (SCA 2010).

Today, smart cards have become an industry standard in terms of identity recognition and management systems. Information and privacy protection, strong ID security, sophisticated “on-card” processing capabilities including: encryption, decryption, biometric matching, electronic signatures, and authenticated as well as authorized information access are all capabilities boasted by smart card technology (SCA 2010).

Additionally, a card carrying digital identity credential is very easy for individuals to understand and use. Smart cards feel like the natural next step in the technology evolution process. Thus, smart card technology provides a strong digital identity verification method eliminating the need to burden users with the complexity, responsibility and risk inherent in substantiating identity via more traditional methods (SCA 2010).

Smart card technology has reached an appropriate level of maturity both in terms of the physical technology itself as well as all required supporting information and computing sub-systems. Additionally, there is a significant level of maturity associated with the requirements, standards and oversight rules and regulations to support a DOD national security based implementation. Smart card technology as applied to a biometric based personnel identification verification system can and should be incorporated into the ARAECS.

D. WORKS CITED

(n.d.). Retrieved 2012 31st-January from Army Space and Missile Defence Command: www.smdc.army.mil/Contracts/BAA/DOD-TechnologyReadinessLevels.doc

National Science and Technology Council. 2006. *Iris Technology Overview.*

DODAF. 2013. *DOD Architecture Framework (DODAF)*. Retrieved October 20, 2013, from https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=55e61d5b-9534-4d20-b97d-9fc6a7eb607f#anchorDef

5000.2R, D. 2002. *DOD 5000.2R "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems Acquisition Programs."* DOD.

8521.01E, D. 2008. *DOD Directive 8521.01E "Department of Defense Biometrics."*

Allan, Roger. 2008. "Biometrics Looks to Solve Identity Crisis," Electronic Design, June 19, 2008.

Benantar, Messaoud. 2006. *Access Control Systems*, New York, Springer Science+Business Media, Inc.

Blanchard, B. S., & Fabrycky, W. J. 2011. *Systems Engineering and Analysis.* Upper Saddle River: Prentice Hall.

Bromba, D. M. 2003. *Biometrics FAQ*. From http://www.bromba.com/faq/biofaqe.htm.

CardLogix Corporation., CardLogix. 2010. Smart Card Security. Retrieved from http://www.smartcardbasics.com/smart-card-security.html.

CardLogix Corporation., CardLogix. 2010. Smart Card Standards. Retrieved from http://www.smartcardbasics.com/smart-card-standards.html.

Cornish, C. G. 2003. *U.S. Naval Mine Warfare Strategy--Analysis of the Way Ahead.*

Defense, D. o. 2006. *Risk Management Guide for DOD Acquisition, Sixth Edition.*

Department of Defense. 2011. *DOD Instruction 8520.03 Identity Authentication for Information Systems.*

Department of the Interior. 2009. Implementing the Smart Card Inoperability Specification . Retrieved from http://www.g4stechnology.com/uploads/G4S/Case-Studies/DEPT-OF-THE-INTERIOR-0611.pdf

Erickson, A. 2008. *A PLA Navy "Assassin's Mace: Chinese Mine Warfare."* U.S. Naval War College.

General Services Administration Office of Government Wide Policy. 2004. Government Smart Card Handbook. Retrieved (2013, November) from http://www.smartcardalliance.org/resources/pdf/smartcardhandbook.pdf

HowStuffWorks, Inc. 2014. What Is A Smart Card? Retrieved from http://www.howstuffworks.com/question332.html.

John, D. Woodward, J. N. 2003. *Biometrics.* New York: McGraw Hill Osborne.

L3 Security and Detection Systems. 2013. CX-Gantry Fact Sheet.

L3 Security and Detection Systems. 2013. ProVision ATD Fact Sheet.

National Science and Technology Council. 2006. *Biometrics Overview.*

National Science and Technology Council. 2006. *Dynamic Signature.*

National Science and Technology Council. 2006. *Face Recognition.* NIST.

National Science and Technology Council. 2006. *Finger Print Technology Overview.*

National Science and Technology Council. 2006. *Hand Geometry.*

National Science and Technology Council. 2006. *Palm Print Recognition.* (NSTC), National Science and Technology Council.

National Science and Technology Council. 2006. *Speaker Recognition.*

National Science and Technology Council. 2006. *Vascular Pattern Recognition.*

PE0602782N: Mine & Exp Warfare Applied Res. 2011. *Appropriation Budget Activity* .

NEUROtechnology, NEUROTEC. 2014. MegaMatcher SDK. Retrieved from http://www.neurotechnology.com/megamatcher.html

NIST Workshop on Storage and Processor Card-Based Technologies, 2003. Interoperability and Card Printing. Retrieved from http://csrc.nist.gov/publications/nistir/IR-7056/Interoperability/Goyet-Interoperability.pdf

Smart Card. 2014. In Wikipedia, The Free Encyclopedia. Retrieved 21:45, April 1, 2014, from http://en.wikipedia.org/w/index.php?title=Smart_card&oldid=602162205

Smart Card Alliance. 2009. Authentication Mechanisms for Physical Access Control. Retrieved January, 2014 from http://www.smartcardalliance.org/resources/lib/PACS_Authentication_20091016.pdf

Smart Card Alliance. 2010. Smart Card Technology and the National Cybersecurity Strategy. Retrieved from http://www.smartcardalliance.org/pages/slideshows-20101111?template=slides

Smart Card Alliance. 2011. Smart Cards and Biometrics. Retrieved (2014, January) from http://www.smartcardalliance.org/resources/pdf/Smart_Cards_and_Biometrics_030111.pdf

U.S. Congress. House of Representatives. Subcommittee on National Security, Homeland Defense, and Foreign Operations. *TSA Oversight Part 2: Airport Perimeter Security, Hearings to National Security Subcommittee*. July 13, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. REQUIREMENTS

(Based on example provided in Blanchard and Fabrycky, p. 96)

1.0 Scope
2.0 Applicable Documents
3.0 Requirements
3.1 System Definition
3.1.1 General Description
3.1.1.1 A system shall be provided for controlling entry of authorized personnel within limited areas. (41M)
3.1.1.2 A system shall be provided for controlling entry of authorized vehicles within limited areas. (41M)
3.1.1.3 A system shall be provided for controlling entry of authorized personnel within exclusion areas. (41M)
3.1.1.4 A system shall be provided for controlling entry of authorized vehicles within exclusion areas. (41M)
3.1.1.5 This paragraph describes the basic capabilities, system requirements, and procedures for an AECS should one be installed at a nuclear weapons storage area or site. (41M)
3.1.1.5.1 The AECS may remove or lessen the impact of the Entry Control's subjective judgment through automated identification. (41M)
3.1.1.5.2 An AECS may provide an integrated capability for entry and circulation control of all personnel authorized entry into areas containing nuclear weapons, systems, and components. (41M)
3.1.1.5.3 Military Departments shall prescribe which levels of AECS are authorized for specific situations (e.g., entry into the limited and exclusion areas). (41M)
3.1.1.5.4 Applicability of a DOD-approved AECS for a specific site shall be made by the responsible commander. (41M)
3.1.1.5.5 Other considerations in planning for an AECS include communications and computer requirements, safety, power, survivability, and interface with other planned security systems. (41M)
3.1.1.5.6 The system must address human engineering requirements in an NBC environment, and extreme weather conditions or environments, day and night. (41M)

3.1.1.6 The system shall control movement of personnel in accordance with the sensitivity, classification, value, and operational importance of the area. (OPNAV)

3.1.1.7 The system shall control movement of vehicles in accordance with the sensitivity, classification, value, and operational importance of the area. (OPNAV)

3.1.2 Operational Requirements (Need, Mission, Use Profile, Distribution, Life Cycle)

3.1.2.1 Entry control system shall be provided for limited areas. (41M)

3.1.2.2 Circulation control system shall be provided for limited areas. (41M)

3.1.2.3 Entry control system shall be provided for exclusion areas. (41M)

3.1.2.4 Circulation system shall be provided for exclusion areas. (41M)

3.1.2.5 Effective control of entry, exit, and internal movement of personnel, material, and vehicles through established limited and exclusion area entry control points and within limited and exclusion areas is required. (41M)

3.1.2.6 Automated or manual entry control procedures shall be employed at limited area boundaries to ensure identification of all personnel prior to entry. (41M)

3.1.2.7 Automated or manual entry control procedures shall be employed at exclusion area boundaries to ensure identification of all personnel prior to entry. (41M)

3.1.2.8 At a minimum, the procedures instituted for limited and exclusion areas shall include: (41M)

3.1.2.8.1 Controlled picture badge system (41M)

3.1.2.8.2 Controlled entry control system (41M)

3.1.2.8.3 Controlled authorization roster (41M)

3.1.2.8.4 Visitor escort system (41M)

3.1.2.8.5 Duress system (41M)

3.1.2.8.6 Inspection system (41M)

3.1.2.9 When an exchange badge system is in use and the badge contains sufficient information to assure identification of the bearer, it may be used in lieu of an entry control or authorization roster. (41M)

3.1.2.10 When an AECS is employed, the authorized personnel access database and automatic event logging capability of the system may be substituted for the entry control or authorization roster. (41M)

3.1.2.11 Except as a temporary expedient for convoys and other special circumstances, entry and exit from a limited or exclusion area shall be at a single point and by one person or driver and vehicle at a time. (41M)

3.1.2.11.1 “The U.S. commander responsible for the weapon(s) may authorize the security force to enter or exit the limited area as a group provided that individual identification is attested to by the group leader, a roster is provided in advance, and vehicle entry and inspections are conducted as provided in paragraph (row 24) of this document (41M)

3.1.2.12 Prescribed entry control procedures may be modified to facilitate realistic, rapid entry or exit into limited or exclusion areas during the response to an actual emergency or related training exercise conducted to demonstrate a team’s or force’s emergency response capability. (41M)

3.1.2.12.1 In any event, the safety and security of nuclear weapons shall not be jeopardized. (41M)

3.1.2.12.2 Other emergency forces may also be allowed rapid entry under the same conditions. (41M)

3.1.2.12.3 Measures shall be implemented to compensate for this modification of normal entry procedures. (41M)

3.1.2.13 Security personnel (posted on watch) inside the limited area shall be notified whenever personnel enter or exit during non-duty hours. (41M)

3.1.2.14 Badges shall be worn in a conspicuous and readily identifiable location on the outer garment at all times while inside the limited and exclusion areas. (41M)

3.1.2.14.1 Badges used exclusively for limited area entry or access must be removed (not displayed) when outside the limited area. (41M)

3.1.2.14.2 Military Departments will define procedures to ensure positive identification of personnel while in these areas when safety considerations prohibit the wearing of such items. (41M)

3.1.2.15 Vehicle Entry Procedures

3.1.2.15.1 All passengers shall exit the vehicle and proceed through the ECP as pedestrians prior to the vehicle entering or exiting the limited and/or exclusion area boundary or ECF entrapment area (41M)

3.1.2.15.2 Only essential Government vehicles or those used for official military duties in lieu of

Government vehicles shall be permitted to operate in limited and exclusion areas. (41M)

3.1.2.15.3 All vehicles shall be inspected by security personnel for unauthorized personnel and readily detectable prohibited and contraband items. (41M)

3.1.2.15.4 Each vehicle shall be given at least a visual inspection of readily accessible areas (e.g., driver and passenger compartments, cargo carrying area, engine compartment, and undercarriage). (41M)

3.1.2.15.5 At Force Protection Conditions (FPCONs) Normal, Alpha, and Bravo; Armed Sentry(ies) (AS) are be assigned as identification checkers at all installation perimeter vehicle Entry Control Points. (OPNAV)

3.1.2.15.5.1 In addition to the armed sentries; unarmed personnel may be assigned as identification checkers to maintain smooth traffic flow at all installation perimeter vehicle Entry Control Points. (OPNAV)

3.1.2.15.6 All vehicles on Navy activities are subject to administrative inspection. (OPNAV)

3.1.2.15.7 No person or group, except as provided in subparagraph 3.1.2.15.7.1, may be exempted from, or singled out for, vehicle inspections. (OPNAV)

3.1.2.15.7.1 Vehicles used by Federal agents (i.e., Federal Bureau .of Investigation, U.S. Secret Service, NCIS, Central Intelligence Agency, Defense Intelligence Agency, Army Criminal Investigation Division, and Air Force Office of Special Investigations) when conducting official business, upon presentation of their special agent credentials when entering or leaving Navy activities, are exempt from administrative inspections

3.1.2.15.8 Vehicles attempting to enter an activity may not be inspected over the objection of the individual. However, the vehicle will not be allowed to enter. (OPNAV)

3.1.2.15.9 Actions carried out during an administrative vehicle inspection include the verification of occupant identity. (OPNAV)

3.1.2.15.10 Actions carried out during an administrative vehicle inspection include the verification of commercial vehicles, the verification of delivery documents (e.g., bill of lading). (OPNAV)

3.1.2.15.11Personnel responsible for the accomplishment or implementation of vehicle control procedures shall be watchful for unauthorized introduction to and removal from the installation government property. (OPNAV)

3.1.2.16 Personnel Entry Procedures

3.1.2.16.1 Upon entering and leaving a limited area all individuals granted unescorted entry authority and their handcarried items shall be subject to inspection by security personnel for readily detectable prohibited materials and contraband items. (41M)

3.1.2.16.2 All individuals being escorted into the area and their hand-carried items shall be inspected by security personnel for readily detectable prohibited materials and contraband items. (41M)

3.1.2.16.3 At limited areas only, inspections of assigned on-duty Security Forces may be carried out separately by the officer or noncommissioned officer in charge of the unit. (41M)

3.1.2.16.4 Federal agents (i.e., Federal Bureau of Investigation, U.S. Secret Service, NCIS, Central Intelligence Agency, Defense Intelligence Agency, Army Criminal Investigation Division, and Air Force Office of Special Investigations) when conducting official business, upon presentation of their special agent credentials when entering or leaving Navy activities, are exempt from administrative inspections. (OPNAV)

3.1.2.16.5 Persons attempting to enter an activity may not be inspected over the objection of the individual. However, these persons will not be allowed to enter. (OPNAV)

3.1.2.16.6 Personnel responsible for the accomplishment or implementation of personnel control procedures shall be watchful for unauthorized introduction to and removal from the installation government property. (OPNAV)

3.1.2.17 Personnel and vehicles directly associated with an ongoing operational or emergency movement of a nuclear weapon(s) are exempt from the inspection requirement upon entering or leaving limited and exclusion areas while delivering, removing, or escorting the nuclear weapon from or to the area. (41M)

3.1.2.17.1 Such persons and vehicles must have been subjected to an inspection and the vehicles maintained sanitized and controlled prior to the start of the movement. They are not exempt from these inspection requirements upon normally entering the area to prepare for a weapon movement or upon departure from the area at the conclusion of the movement. This exemption is only applicable while directly carrying or escorting nuclear weapons into or out of a limited or exclusion area. (41M)

3.1.2.18 Persons entering nuclear weapon limited and exclusion areas under U.S. Treaty obligations will be subjected to the provisions of such treaties and, if so stipulated as a condition of the treaty, be exempted from the inspection requirements. (41M)

3.1.2.18.1 U.S. commanders responsible for the weapon(s) should consider and, if deemed necessary, implement mitigation strategies to limit vulnerabilities (if any) to the weapon(s). Under no circumstances will a U.S. Treaty inspector be allowed entry to an exclusion area unless a suitable two-person team is present. (41M)

3.1.2.19 Installation Commanding Officers (ICOs) shall ensure that the minimum security measures are employed for restricted areas to include a clearly defined protected perimeter. (OPNAV)

3.1.2.20 ICOs shall ensure that the minimum security measures are employed for restricted areas to include - controlled access limited to those with appropriate clearance and “need-to-know,” (OPNAV)

3.1.2.21 ICOs shall ensure that the minimum security measures are employed for restricted areas to include establishment of a personnel identification system, (OPNAV)

3.1.2.22 ICOs shall ensure that the minimum security measures are employed for restricted areas to include performance of checks for unauthorized entry every 8 hours during normal working hours. (OPNAV)

3.1.2.23 ICOs shall ensure that the minimum security measures are employed for restricted areas to include performance of checks for unauthorized entry every 4 hours after normal working hours. (OPNAV)

3.1.2.24 ICOs shall ensure that the minimum security measures are employed for restricted areas to include designation of a response force. (OPNAV)

3.1.3 Maintenance Concept

3.1.4 Functional Analysis and System Definition

3.1.5 Allocation of Requirements

3.1.6 Functional Interfaces and Criteria

3.1.6.1 Units will leverage existing force protection equipment and procedures and adapt them for use at limited and exclusion area entry points. (41M)

3.1.6.2 The AECS shall be integrated into the overall site security operations. (41M)

3.1.6.3 The AECS shall provide alarms to existing IDS annunciators. (41M)

3.1.6.4 The AECS shall be capable of accepting alarms from IDS. (41M)

3.1.6.5 Upgrades to existing access controls systems shall have ability to provide rapid electronic authentication to Federal and DOD authoritative databases, including DEERS. (OPNAV)

3.2 System Characteristics

3.2.1 Performance Characteristics

3.2.1.1 AECS shall have the capability to accept and process the covert entry of a duress code by any system user. (41M)

3.2.1.1.1 The system shall alert all other on-line operators of the duress condition. (41M)

3.2.1.2 Authentication of an individual's authorization to enter the area shall be accomplished using one of three separate levels of personal identification, as described in paragraph 5. h. (2) (a) 1., 2., and 3. (Automated Entry -> System Performance Requirements-> Identification Authentication Process->Levels 1, 2 and 3) of this Enclosure. (41M)

3.2.1.3

3.2.2 Physical Characteristics

3.2.2.1 Where AECS equipment is employed, separate exit lanes with the appropriate equipment shall be provided to control exit from the area. (41M)

3.2.2.1.1 Final exit from the limited and exclusion area shall be under positive control of the EC. (41M)

3.2.2.2 Controlled picture badges shall be provided for personnel authorized unescorted entry to limited and exclusion areas. (41M)

3.2.2.2.1 Positive identification shall be accomplished. (41M)

3.2.2.2.2 The distinctive badge system shall be changed when any event or circumstance indicates the possibility of compromise of the badge system. (41M)

3.2.2.2.3 The badge shall have distinctive markings that can be easily recognized by an authorized individual observing the badge. (41M)

3.2.2.2.4 When an AECS is employed, an electronically generated badge may be used. (41M)

3.2.2.2.4.1 These badges shall incorporate a means of recording information required by the automated equipment. (41M)

3.2.2.2.4.2 When AECS is in use, badge exchange procedures are not required. (41M)

3.2.2.2.5 Badge production shall incorporate measures that ensure badges cannot be easily counterfeited. (41M)

3.2.2.3 Automated means of inspecting personnel and hand carried items may be used in place of manual procedures. (41M)

3.2.2.4 DOD CAC shall be principal card enabling access to buildings, facilities, installations, ships, and controlled spaces. (OPNAV)

3.2.2.4.1 Supplemental badging shall be used for additional level of security not presently afforded by the CAC. (OPNAV)

3.2.2.5 Supplemental badging shall be used for AECSS incorporating technology that is not supported by the CAC.

3.2.3 Effectiveness Requirements

3.2.3.1 The number of personnel authorized entry to limited areas shall be kept to a minimum. (41M)

3.2.3.2 The number of personnel authorized entry to exclusion areas shall be kept to a minimum. (41M)

3.2.4 Reliability

3.2.4.1 Upgrades to existing access controls systems shall include an emergency power source. (OPNAV)

3.2.5 Maintainability

3.2.6 Security

3.2.6.1 The U.S. commander responsible for the weapon(s) may permit unescorted entry into limited areas to those personnel not certified in the U.S. PRP as described below. (41M)

3.2.6.1.1 Entry into limited areas may be given to U.S. military personnel and U.S. DOD civilian employees who have a need to know and at least a Confidential security clearance. (41M)

3.2.6.1.2 Entry into limited areas may be given to employees of U.S. contractors engaged in a related classified contract, provided such employees have a Confidential security clearance. (41M)

3.2.6.2 All personnel not otherwise specified in paragraphs 3.2.6.1.1 and 3.2.6.1.2 of this document shall be escorted inside limited and exclusion areas. (41M)

3.2.6.3 If the entry is to the limited area, the U.S. escort shall have unescorted entry authority into the limited area. (41M)

3.2.6.4 If the entry is to the exclusion area, the U.S. escort shall have unescorted entry authority into the exclusion area. (41M)

3.2.6.5 Escorts for exclusion areas must also be certified through the PRP (or host-nation equivalent at WS3 installations). The U.S. commander responsible for the weapon(s), as part of the entry authorization process, decides whether or not to arm the escorts based on local propriety, threat, and weapon systems vulnerabilities at the time of the entry. (41M)

3.2.6.6 Personnel performing escort duties shall not be assigned other duties. The intent is that persons performing escort duties are not tasked to perform any other functions so they may fully concentrate on the task of properly providing surveillance and control over the person(s) under escort. Inside an exclusion area where a two-person team is required and the sole responsibility of that two-person team is to be present to meet the two-person rule, one person from the two-person team may act as the escort official provided that person has escort authority, the two-person team is familiar enough with the task to be performed to detect an unauthorized act, and the team is performing no other task except providing surveillance and control over the person(s) under escort. In cases where the responsible commander has determined that arming of escorts is not necessary, DOD contractors who meet all other requirements are allowed to perform as escorts. (41M)

3.2.6.7 At sites located in the United States, DOD civilian personnel having at least a Confidential security clearance may perform escort duties within limited areas. (41M)

3.2.6.8 The ratio of personnel to be escorted to the number of escorting personnel shall be such that escorting personnel can satisfactorily perform continuous surveillance and control. (41M)

3.2.6.8.1 Since this number is a function of the task(s) to be performed and the physical layout of the area or facility at which the escort is performed, the escort official is responsible for determining and, as necessary, limiting the number of people under escort control. While the Military Departments may prescribe an upper limit on the number, the escort official is responsible for determining if a lower limit is more appropriate for the task, area, or facility. (41M)

3.2.6.9 A system shall be instituted by which personnel who are permitted unescorted entry to limited and exclusion areas, and for those who control entry into, vouch for, or escort visitors into a limited or exclusion area, can covertly communicate a situation of duress to other personnel. (41M)

3.2.6.9.1 Only those personnel with a need to know shall have access to duress codes. (41M)

3.2.6.9.2 The duress code shall be changed as frequently as is necessary to assure code integrity. (41M)

3.2.6.9.3 The duress communication shall be oral or electronic, or both. (41M)

3.2.6.10 Vehicles and material handling equipment remaining in limited or exclusion areas after duty hours shall be secured to assure that they are not readily usable by a hostile force. (41M)

3.2.6.11 No vehicle or handling equipment shall be parked within the inner or outer clear zone of the limited area. (41M)

3.2.6.12 Signs shall be displayed, except where host-nation laws are sufficient requiring removal of ignition keys and/or immobilization of unattended vehicles and materials and material handling equipment parked within or just outside of limited or exclusion areas so they cannot be readily used by a hostile force. (41M)

3.2.6.13 A procedure shall be established for prompt removal of an individual's authorization to enter the area upon reassignment, transfer, change in status within the PRP or termination or or when an individual's access is suspended, revoked, or downgraded to a level lower than required. (41M)

3.2.6.14 Physical security protection shall be established and continuously maintained for all devices and equipment that constitute the AECS. (41M)

3.2.6.14.1 The level of protection may vary depending on the type of devices and equipment being protected with the basic intent of using the security controls already in effect within the facility. (41M)

3.2.6.15 Locations where authorization data, card encoded data, and personal identification or verification data is entered, stored, processed, or recorded shall be protected so that the integrity of the entry control system is not compromised. (41M)

3.2.6.16 Upgrades to existing access controls systems shall meet Federal Information Processing Standard 201. (OPNAV)

3.2.6.17 Each Navy activity shall establish a system to check restricted areas entry and departure points by occupants/users in an attempt to detect deficiencies of security standards. (OPNAV)

3.2.6.18 Each Navy activity shall establish a system to check restricted areas entry and departure points by occupants/users in an attempt to detect violations of security standards. (OPNAV)

3.2.7 Supportability

3.2.8 Transportability/Mobility

3.2.9 Flexibility

3.2.10 Sustainability

3.2.11 Usability (Human Factors)

3.3 Design and Construction

3.3.1 CAD/CAM Requirements

3.3.2 Materials, Processes, and Parts

3.3.3 Mounting and Labeling

3.3.4 Electromagnetic Radiation

3.3.5 Safety

3.3.6 Interchangeability
3.3.7 Workmanship
3.3.8 Testability
3.3.9 Economic Feasibility

3.4 Documentation/Data

3.5 Logistics

3.5.1 Maintenance Requirements
3.5.2 Supply Support
3.5.3 Test and Support Equipment
3.5.4 Personnel and Training

3.5.4.1 All escorts shall be periodically trained and certified capable of escort duties and responsibilities. (41M)

3.5.5 Facilities and Equipment

3.5.5.1 Level 1: Personal Identification Card or Badge. Level 1 requires an identification card coded for each individual and a card reader. The card or badge shall use embedded sensors, integrated circuits, magnetic strips, or other means of encoding data resistant to tamper or modification that identifies the facility and the individual to whom the card is issued. (41M)

3.5.5.2 Level 2: Identification Card and Personal Identification Number (PIN). This level requires an identification card and a PIN. The PIN shall be separately entered into the system by each individual using a keypad device. (41M)

3.5.5.2.1 The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. (41M)

3.5.5.2.2 The PIN shall be changed when it is believed to have been compromised or threatened with compromise. (41M)

3.5.5.3 Level 3: Identification Card, PIN, and Personal Identity Verification (PIV). This level requires an identification card, a PIN, and a PIV. PIVs (biometric identifiers) identify an individual by some unique personal characteristic. (41M)

3.5.5.4 Card readers, keypads, communication, or interface devices located outside the entrance to a limited area (or exclusion area when the limited and exclusion area boundary are the same) shall have tamper resistant enclosures, be securely fastened to a wall or other structure, and be protected by a tamper alarm. (41M)

3.5.5.5 Control panels located within a limited area shall require only the minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. (41M)

3.5.5.6 Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate area cannot observe the selection of input numbers. (41M)

3.5.5.7 Future AECS installations and modifications or upgrades shall use scramble keypad technology. (41M)

3.5.5.8 Systems that use transmission lines to carry access authorization, personal identification, or verification data between devices and equipment located outside the limited area shall receive a minimum of Class I line supervision. (41M)

3.5.6 Packaging, Handling, Storage and Transportation

3.5.7 Computer Resources (Software)

3.5.8 Technical Data/Information

3.5.8.1 A record of manual or automated entry shall be maintained of all personnel granted access to exclusion and limited areas. (41M)

3.5.8.1.1 Records of entry are a control measure to identify personnel and for use during emergencies requiring evacuation, to ensure all personnel have been evacuated. However, this does not apply to limited areas where Security Forces can immediately discern, or in exclusion areas where vouching authorities can determine, that the area is completely evacuated by visual examination.(41M)

3.5.8.2 Duress codes shall be appropriately classified and controlled. (41M)

3.5.8.3 Where AECS equipment is employed exit from the area shall be logged. (41M)

3.5.8.4 A listing and description of prohibited items shall be provided to the security force by the appropriate logistics organization. (41M)

3.5.8.4.1 Designated items may be exempted from this inspection. (41M)

3.5.8.4.1.1 Such exemptions shall be approved by the Military Service designated commander and kept to an absolute minimum commensurate with operational requirements. (41M)

3.5.8.5 ICOs shall ensure that the minimum security measures are employed for restricted areas to include maintenance of access list and visit log documentation. (OPNAV)

        - 3.5.9 Customer Services
    - 3.6 Producibility
    - 3.7 Disposability
    - 3.8 Affordability
- 4.0 Test and Evaluation
- 5.0 Quality Assurance Provisions
- 6.0 Distribution and Customer Service
- 7.0 Retirement and Material Recycling/Disposal

LIST OF REFERENCES

Blanchard, B. S., and W. J. Fabrycky. 2011. *Systems Engineering and Analysis*. Upper Saddle River: Prentice Hall.

Cornish, Gregory J. 2003. *U.S. Naval Mine Warfare Strategy—Analysis of the Way Ahead*. Research Project, U.S. Army War College.

Department of Defense. 2006. *Risk Management Guide for DOD Acquisition*, 6th ed. Arlington, VA: Department of Defense.

———. 2009. *DOD Nuclear Weapons Security Manual*. DOD S-5210.41-M. Arlington, VA: Department of Defense.

Department of Navy. 2009. Navy Physical Security and Law Enforcement Manual. OPNAVINST 5530.14E w/CH1. Arlington, VA: Department of Defense.

———. 2013. DON Nuclear Weapons Roles and Authorities. SECNAVINST 8120.1A. Arlington, VA: Department of Defense.

Forsberg, Kevin; Harold Mooz, and Howard Cotterman. 2005. Visualizing Project Management, 3rd ed. New York: J. Wiley & Sons.

Naval Criminal Investigative Services Memo. 2011. Department of the Navy Implementation of HSPD-12. Ser N09N2/11U213200.

Strategic Systems Programs. 2013. *Command Risk Management*. SSPINST 5200.15. Washington, DC: Strategic Systems Programs.

Strategic Systems Programs. 2013. *Internal Fiscal Year and Program Objective Memorandum Strategic Systems Program and Budget Review*. SSP Notice 7100. Washington, DC: Strategic Systems Programs.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California